FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA

UNIVERSIDAD NACIONAL DE CÓRDOBA

TESIS DOCTORAL

Métricas sobre grupos y anillos con aplicaciones a la teoría de códigos

Autor:

Maximiliano G. Vides

Director:

Dr. Ricardo A. Podestá

2018

Resumen

Tradicionalmente la Teoría de Códigos se ocupó de construir y analizar códigos sobre cuerpos finitos. Con el tiempo, también comenzaron a considerarse códigos sobre estructuras algebraicas más generales, como anillos, módulos y grupos. Esto llevó a la necesidad de considerar nuevas métricas, además de la clásica métrica de Hamming, más adecuadas para cada una de esas estructuras.

En este trabajo, estudiaremos el espacio de métricas sobre grupos y anillos, en base a equivalencias, de las cuales podremos obtener propiedades generales de métricas especificas de interés para la Teoría de Códigos. Además estudiaremos los grupos de simetrías de métricas, los cuales nos permitirán decidir la existencia o no de isometrías entre espacios con estructuras distintas, obteniendo generalizaciones del conocido mapa de Gray. En particular, estudiaremos las métricas poset; y en el caso de posets jerárquicos, daremos una descripción de su grupo de simetrías, sus identidades de MacWilliams respectivas y describiremos algunas nuevas isometrías obtenidas.

Palabras clave: Códigos, Métricas, Distancias, Grupos, Anillos, Isometrías, Esquemas de asociación, Anillos de Schur.
2010 Mathematics subject Classification:: 11T71, 05E30, 05E18.

Abstract

Traditionally, Coding Theory was occupied with building and analyzing codes over finite fields. Over time, they also began to be considered codes on more general algebraic structures, such as rings, modules and groups. This led to the need to consider new metrics, in addition to the classic Hamming metric, more suitable for each of those structures.

In this paper, we will study the space of metrics on groups and rings, based on equivalences, from which we can obtain properties of specific metrics of interest for Coding Theory. In addition, we will study the symmetry groups of metrics, which will allow us to decide the existence or not of isometries between spaces with different structures, obtaining generalizations of the familiar map of Gray. In particular, we will study the poset metrics; and in the case of hierarchical posets, we will give a description of their group of symmetries, their respectives MacWilliams Identities and we will describe some new isometries obtained.

Palabras clave: Codes, Metrics, Distances, Groups, Rings, Isometries, Association Schemes, Schur Rings.
2010 Mathematics subject Classification:: 11T71, 05E30, 05E18.

Agradecimientos

En primer lugar quiero agradecer a mi director, Dr. Ricardo Podestá, por su confianza en mi trabajo, y por toda su ayuda durante la realización de este trabajo, tanto en el plano académico como personal.

A toda mi familia, mamá, hermana, primos y tios por siempre estar cuando los necesite, y principalmente porque siempre confiaron en mi. Especialmente a mi padre, que siempre estará en mis pensamientos. A mi novia Taianara por todo su amor, por acompañarme, ayudarme y brindarme todo su apoyo durante este tiempo.

Agradecer también a todas aquellas personas que conocí a lo largo de estos años en FaMAF, amigos, compañeros de clase, compañeros de oficina, con los que compartí muy buenos momentos, como tardes de estudio, juntadas, etc, de los cuales siempre tendré buenos recuerdos. También quiero agradecer a FaMAF y al CIEM por haberme brindado el lugar de trabajo, a los docentes y personal administrativo por su buena predisposición para ayudar siempre. En particular a mi comisión asesora y a mis jurados de tesis, por su inconmensurable ayuda y buena disposición para conmigo.

Índice general

Introducción

El estudio de códigos sobre anillos y grupos finitos tomó gran importancia luego de que, Nechaev, en [44], y más tarde Hammons et al. en [22], demostraran que tanto los códigos de Kerdock y los códigos Preparata son imágenes bajo cierta isometría (el mapa de Gray) de algunos códigos lineales sobre $\mathbb{Z}_4$ que son duales entre sí. Mas aún, gracias a este último trabajo, las descripciones de estos códigos se vuelven más simples utilizando las propiedades de los correspondientes códigos lineales sobre $\mathbb{Z}_4$ y lograron dar una explicación para la dualidad entre estas dos familias. Tal fue su importancia, que desde entonces se ha abierto la puerta al estudio de muchos códigos lineales sobre $\mathbb{Z}_4$ y, en general, ha llevado a analizar códigos sobre $\mathbb{Z}_{p^s}$, y luego sobre anillos en general.

Intentando generalizar esta idea y teniendo en cuenta la utilidad de la métrica de Lee, se consideró también la idea de utilizar métricas distintas a la de Hamming, más adecuadas para cada anillo. De esta manera surgieron muchos tipos de métricas, como la métrica homogénea, la métrica rango, métricas de Lee generalizadas; cada una para un uso específico, generalmente relacionado con isometrías sobre el espacio de Hamming para determinar códigos no lineales con mejores parámetros como en el caso de las familias de Kerdock y Preparata.

En [49], Delsarte se percató de que las relaciones de distancia en el espacio de Hamming $(\mathbb{F}_q^n, d_{Ham})$ daban origen a un *esquema de asociación*, ahora conocido como el esquema de Hamming, y que muchos de los resultados obtenidos en la teoría de códigos provenían de la teoría de esquemas de asociación, en particular, la identidad de MacWilliams.

Estructura de trabajo

La idea principal será tratar de determinar una clasificación de métricas sobre grupos y anillos, relacionada con la teoría de esquemas de asociación para el uso en la teoría de códigos. Tal clasificación nos permitirá determinar la existencia o no de isometrías entre distintos espacios, permitiendo generalizar los conceptos previos de las isometrías de Gray, además de permitir determinar que tipos de métricas serán más adecuadas para usos específicos.

A continuación se describirá la estructura de este trabajo para facilitar su lectura y comprensión.

1. Preliminares. Se darán definiciones básicas de la Teoría de Códigos, que servirán como introducción al tema, así como resultados conocidos en las áreas de grafos, esquemas de asociación, anillos de Schur y grupos de permutaciones, que se usarán en los siguientes capítulos.

2. Métricas En este capítulo se comenzará con el estudio de métricas sobre grupos y anillos, introduciendo el concepto de grupo de simetrías de una distancia, que sera fundamental para la clasificación de métricas. Además, se analizará la relación entre métricas y otros conceptos como esquemas de asociación, grafos, grupos de permutaciones y anillos de Schur.

3. Métricas poset. Aplicaremos los conceptos de los capítulos anteriores al estudio de las denominadas *métricas poset*. En el caso de que el poset sea jerárquico calcularemos explícitamente el grupo de simetrías de la métrica.

4. Dualidad e identidades de MacWilliams. Definiremos el concepto de dualidad de una métrica y consideraremos la existencia de una identidad de MacWilliams para las distintas clases de métricas, que relacione el enumerador de peso de un código con el enumerador de su código dual. En particular, daremos una descripción recursiva para obtener tales identidades para métricas que provienen de posets jerárquicos.

5. Isometrías. En este capítulo se estudiará la existencia de isometrías entre distintos grupos y anillos, tratando el problema de generalizar la famosa isometría de Gray. También analizaremos los casos conocidos de generalizaciones de los mapas de Gray. En particular obtendremos una forma de generar nuevas isometrías.

6. Conclusión. Se dará un breve resumen de los resultados más importantes del trabajo, así como un comentario sobre los posibles usos y aplicaciones dentro de la Teoría de Códigos, llevando a nuevas investigaciones.

La idea central de este trabajo es estudiar métricas invariantes sobre grupos y anillos. Para esto, en el capítulo 2 comenzamos definiendo el espacio $\mathcal{M}(G)$ de métricas invariantes de un grupo G. Las métricas más utilizadas y que tienen mejores propiedades, suelen están relacionadas con esquemas de asociación; por esta razón seria de gran importancia saber cuales son las métricas que son de este tipo. Para ello, definimos un tipo de equivalencia de métricas en $\mathcal{M}(G)$, en base a su grupo de simetrías, que en el caso que G sea abeliano, nos permite identificar cada una de esas clases con un esquema de asociación. De esta forma, obteniendo una correspondencia entre métricas sobre G y esquemas de asociación de Cayley (o equivalentemente S-anillos simétricos schurianos sobre G)

$$\begin{array}{ccc} \{\Gamma\text{-clases de métricas}\} & \longleftrightarrow & \{\text{Particiones schurianas simétricas}\} \\ \updownarrow & & \updownarrow \\ \{\text{Grupos de simetrías}\} & \longleftrightarrow & \{\text{S-anillos simétricos schurianos}\} \end{array}$$

Para algunos grupos G estas relaciones nos permite determinar todos los tipos de métricas que inducen un esquema de asociación. En particular, en el caso $G = \mathbb{Z}_p$ los Teoremas 2.3.15 y 2.3.16, obtenemos la clasificación de métricas schurianas de $\mathbb{Z}_p$. Además, para el caso $G = \mathbb{Z}_n$, vemos que toda métrica de Schur se obtiene en base a construcciones de métricas de Schur descriptas anteriormente. Esto puede verse en la sección de Apéndices.
Luego utilizamos todo este marco, para estudiar un tipo de métricas de gran relevancia en los últimos tiempos, las métricas poset. En particular, para el caso de posets jerárquicos logramos determinar el grupo de simetrías (Teorema 3.3.3):

Sea $P = \mathbb{H}(n; n_1, \ldots, n_k)$ un poset jerárquico, entonces se tiene que

$$\Gamma(\mathbb{F}_q^n, d_P) \simeq ((\mathbb{S}_q \wr \mathbb{S}_{n_1}) \wr \cdots \wr (\mathbb{S}_q \wr \mathbb{S}_{n_k})).$$

En el capítulo 4, utilizando la conexión entre métricas y esquemas de asociación visto en el capítulo 2, analizamos la dualidad entre métricas, definiendo así, para cada métrica $d \in \mathcal{M}(G)$ una métrica dual d^*. Para las construcciones de métricas vistas, damos las correspondientes métricas duales en el Teorema 4.1.11. Este concepto de dualidad nos permite utilizar las identidades de MacWilliams de la teoría de esquemas de asociación para obtener una relación entre los enumeradores de peso de un código con respecto a la métrica d y su código dual con respecto a d^*. En particular, para el caso de las métricas posets, logramos dar una descripción alternativa a las ya conocidas, de las identidades de MacWilliams correspondientes (Teorema 4.2.13).

Finalmente, en el capítulo 5 vemos la relación entre isometrías y grupos de simetrías. En este caso, el estudio del espacio $\mathcal{M}(G)$ nos permite determinar en que casos existen isometrías entre espacios

métricos. Por ejemplo, obtenemos otra prueba de los resultados ya conocidos sobre la no existencia de isometrías del espacio de Hamming (F_q^n, d_{Ham}) con algún espacio de la forma $(\mathbb{Z}_{q^n}, d)$ (Teoremas 5.2.3 y 5.2.5). También obtenemos resultados sobre la existencia de isometrías de $\mathbb{Z}_{p^k}$ en espacios de Hamming, para $k < n$ (Teoremas 5.3.5 y 5.3.7). Por último, en el Teorema 5.5.3, construimos una isometría entre el espacio (F_q^n, d_{RT}) y $(\mathbb{Z}_{q^n}, d_q)$.

Capítulo 1

Preliminares

En este capítulo daremos las nociones básicas de la teoría de códigos clásica, sobre $\mathbb{F}_q$. Luego veremos definiciones y resultados sobre grafos de Cayley, esquemas de asociación, álgebras de grupo y anillos de Schur. También veremos algunas relaciones entre estos conceptos, que luego utilizaremos durante todo este trabajo.

1.1. Teoría de Códigos

En esta sección se verán algunos conceptos básicos de la Teoría de Códigos, tales como definiciones que servirán de lenguaje para los siguientes capítulos, notaciones, conceptos elementales, los cuales pueden encontrarse en la mayoría de libros relacionados al tema. Para la teoría clásica de códigos sobre cuerpos finitos pueden verse [38] y [57] y para el caso de códigos sobre anillos, se recomienda el trabajo de Jay Wood [66].

Definición 1.1.1. Sea $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$ un conjunto finito, denotado como el **alfabeto del código**. Una **palabra de longitud** n ó n-**cadena** es una sucesión de n símbolos de $\mathcal{A}$, que serán denotados de la forma

$$a_{i_1}a_{i_2}\cdots a_{i_n}, \quad \text{ó} \quad (a_{i_1}, a_{i_2}, \ldots, a_{i_n}), \quad \text{con } a_{i_k} \in \mathcal{A}.$$

Denotaremos por $\mathcal{A}^n$ al conjunto de todas las palabras de longitud n, y sea

$$\mathcal{A}^* = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n$$

Cualquier subconjunto $\mathcal{C} \subset \mathcal{A}^*$ será llamado un **código**, además si $\mathcal{C} \subset \mathcal{A}^n$ diremos que es un **código de bloque** q-**ario**, y cada palabra en $\mathcal{C}$ será llamada una **palabra-código**. Si $\mathcal{C} \subset \mathcal{A}^n$ contiene M palabras-código se dirá que $\mathcal{C}$ tiene longitud n y tamaño M, o que es un (n, M)-código.

En general, los códigos mas estudiados son los códigos de bloque q-arios, a los cuales nos refe-

riremos siempre en este trabajo. Por simplicidad, nos referiremos a las palabras-código simplemente por palabras.

Definición 1.1.2. Sean **a** y **b** palabras de la misma longitud n, sobre el mismo alfabeto $\mathcal{A}$. La **distancia de Hamming** entre **a** y **b** se define como

$$d(\mathbf{a},\mathbf{b}) = |\{i \in [1,n] : a_i \neq b_i\}|,$$

es decir el número de coordenadas en que difieren **a** y **b**.

Si el alfabeto $\mathcal{A}$ contiene un símbolo 0 (por ejemplo si $\mathcal{A}$ es un cuerpo finito o un anillo), el **peso de Hamming** de una palabra $\mathbf{c} \in \mathcal{C}$, denotado $wt(\mathbf{c})$, se define por

$$w(\mathbf{c}) = d(\mathbf{c},\mathbf{0}),$$

donde $\mathbf{0}$ denota la palabra con todos sus símbolos iguales a 0.

Proposición 1.1.3. *Sea $\mathcal{A}^n$ el conjunto de todas las palabras de longitud n sobre el alfabeto $\mathcal{A}$. Entonces la distancia de Hamming $d : \mathcal{A}^n \times \mathcal{A}^n \longrightarrow \mathbb{N}_0$ satisface las siguientes propiedades:*

(i) $d(\mathbf{a},\mathbf{b}) \geq 0$, *y* $d(\mathbf{a},\mathbf{b}) = 0 \iff \mathbf{a} = \mathbf{b}$,

(ii) $d(\mathbf{a},\mathbf{b}) = d(\mathbf{b},\mathbf{a})$,

(iii) $d(\mathbf{a},\mathbf{b}) \leq d(\mathbf{a},\mathbf{c}) + d(\mathbf{c},\mathbf{b})$,

para todo $\mathbf{a},\mathbf{b},\mathbf{c} \in \mathcal{A}^n$. *Por lo tanto $(\mathcal{A}^n, d)$ es un espacio métrico.*

Definición 1.1.4. La **distancia mínima** de un código $\mathcal{C}$ se define como:

$$d(\mathcal{C}) = \min_{\substack{\mathbf{c},\mathbf{d}\in\mathcal{C} \\ \mathbf{c}\neq\mathbf{d}}} d(\mathbf{c},\mathbf{d}).$$

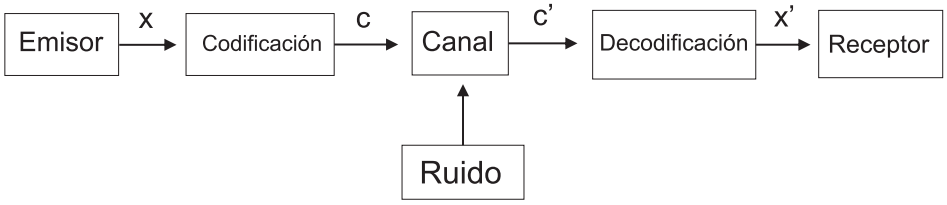
Un (n,M,d)-**código** será un código de longitud n, tamaño M y distancia mínima d.

El **peso mínimo de Hamming** de un código $\mathcal{C}$, denotado $wt(\mathcal{C})$, será

$$w(\mathcal{C}) = \min_{\substack{\mathbf{c}\in\mathcal{C} \\ \mathbf{c}\neq 0}} w(\mathbf{c})$$

Imaginemos que queremos enviar un mensaje por un canal de comunicación, cuyas características dependen de la naturaleza del mensaje a ser enviado (i.e. sonido, imagen, datos). En general, hay que hacer una traducción entre el mensaje original (o palabra fuente) **x** y el tipo de mensaje **c** que el canal está capacitado para enviar (palabras código). Este proceso se llama codificación. Una vez codificado el mensaje, lo enviamos a través del canal y nuestro intermediario (el receptor) recibe un mensaje codificado (palabra recibida) posiblemente erróneo, ya que en todo proceso de comunicación hay ruido

e interferencias. El mensaje recibido $\mathbf{c}'$ es traducido nuevamente a términos originales como $\mathbf{x}'$, es decir, es decodificado.



Sea $\mathcal{C} \in \mathcal{A}^n$. Supongamos que la palabra $\mathbf{c} \in \mathcal{C}$ es enviada a través del canal, y la palabra $\mathbf{c}' \in \mathcal{A}^n$ es recibida, la **decodificación por distancia mínima** consiste en elegir una palabra $\mathbf{c}^* \in \mathcal{C}$ cuya distancia $d(\mathbf{c}^*, \mathbf{c}')$ sea mínima (i.e. que el mensaje recibido sea lo mas fiel posible a la palabra enviada).

Definición 1.1.5. Sea $\mathcal{C}$ un (n, M)-código. Denotaremos por A_i al número de palabras de peso i en $\mathcal{C}$ para $0 \leq i \leq n$. La **distribución de peso** de $\mathcal{C}$ serán los números $A_0, \ldots, A_n$ y el polinomio

$$W_{\mathcal{C}}(x) = \sum_{k=0}^{n} A_k x^k$$

se denominará **enumerador de peso** de $\mathcal{C}$.

También en muchas ocasiones será más útil pensar en el enumerador de peso como un polinomio homogéneo de grado n de la forma:

$$W_{\mathcal{C}}(x, y) = \sum_{k=0}^{n} A_k x^{n-k} y^k.$$

Códigos lineales

Para el estudio de códigos es útil dotar al alfabeto de cierta estructura algebraica. Es común considerar el alfabeto $\mathcal{A}$ como $\mathbb{F}_q$, el cuerpo finito de q elementos. Recordemos que $\mathbb{F}_q$ es único salvo isomorfismos y que $q = p^r$ para algún primo p y $r \in \mathbb{N}$. Por lo tanto, el conjunto $\mathcal{A}^n$ puede identificarse naturalmente con el espacio vectorial $\mathbb{F}_q^n$ mediante la asignación

$$\begin{aligned} \mathcal{A}^n &\longleftrightarrow \mathbb{F}_q^n \\ a_1 a_2 \ldots a_n &\longleftrightarrow (a_1, a_2, \ldots, a_n). \end{aligned}$$

Definición 1.1.6. Un código $\mathcal{C} \subset \mathbb{F}_q^n$ es un **código lineal** si es un subespacio de $\mathbb{F}_q^n$. Si $\mathcal{C}$ tiene dimensión k sobre $\mathbb{F}_q$, diremos que es un $[n, k]$-**código**, y si $\mathcal{C}$ tiene distancia mínima d, decimos que es un $[n, k, d]$-**código**.

Dualidad

En esta sección se tratará la Identidad de MacWilliams, una herramienta fundamental en la Teoría de Códigos, que permite relacionar el enumerador de peso de un código lineal $\mathcal{C}$ con el enumerador de su código dual $\mathcal{C}^{\perp}$.

El espacio vectorial $\mathbb{F}_q^n$ posee un producto interno natural, dados $\mathbf{a} = a_1 \dots a_n$ y $\mathbf{b} = b_1 \dots b_n$ el **producto escalar** de $\mathbf{a}$ y $\mathbf{b}$ es

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \cdots + a_n b_n.$$

Definición 1.1.7. Sea $\mathcal{C}$ un $[n,k]$-código. El subespacio

$$\mathcal{C}^{\perp} = \{\mathbf{a} \in \mathbb{F}_q^n \,:\, \mathbf{a} \cdot \mathbf{c} = 0 \ \ \forall \mathbf{c} \in \mathcal{C}\}$$

será llamado el **código dual** de $\mathcal{C}$.

Algunas de las propiedades que cumple el código dual, son las siguientes.

Proposición 1.1.8. *Sea $\mathcal{C}$ un $[n,k]$-código sobre $\mathbb{F}_q$, entonces $\mathcal{C}^{\perp}$ cumple*

(i) $\mathcal{C}^{\perp} \subseteq \mathbb{F}_q$,

(ii) $\mathcal{C}^{\perp}$ *es un código lineal de longitud n,*

(iii) $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

(iv) $dim(\mathcal{C}^{\perp}) = n - dim(\mathcal{C})$ $\quad$ *(ó* $|\mathcal{C}||\mathcal{C}^{\perp}| = |\mathbb{F}_q^n| = q^n$*).*

Teorema 1.1.9 (MacWilliams)**.** *Sea $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_q$, $\mathcal{C}^{\perp}$ su dual y sean*

$$W_{\mathcal{C}}(x) = \sum_{k=0}^{n} A_k x^k \qquad y \qquad W_{\mathcal{C}^{\perp}}(x) = \sum_{k=0}^{n} A_k^{\perp} x^k$$

los enumeradores de peso de $\mathcal{C}$ y $\mathcal{C}^{\perp}$ respectivamente, entonces

$$W_{\mathcal{C}^{\perp}}(x) = \frac{1}{|\mathcal{C}|}(1+(q-1)x)^n W_{\mathcal{C}}\left(\frac{1-x}{1+(q-1)x}\right). \tag{1.1}$$

Equivalentemente

$$A_k^{\perp} = \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n} A_i K_k^n(i), \tag{1.2}$$

donde $K_k^n(x)$ es el polinomio de Krawtchouk de orden n y grado k.

Además si consideramos el enumerador de peso, como un polinomio homogéneo de grado n en las variables x, y tenemos la siguiente relación

$$W_{\mathcal{C}}(x,y) = \frac{1}{|\mathcal{C}^{\perp}|} W_{\mathcal{C}^{\perp}}(x+(q-1)y, x-y), \tag{1.3}$$

en particular, en el caso binario se tiene la relación

$$W_{\mathcal{C}}(x,y) = \frac{1}{|\mathcal{C}^{\perp}|} W_{\mathcal{C}^{\perp}}(y+x, y-x), \tag{1.4}$$

1.2. Grafos de Cayley

En esta sección daremos las nociones básicas sobre grafos de Cayley, que usaremos mas adelante. Si G es un grupo, denotaremos por e a su elemento identidad. Un subconjunto S de G se dice *simétrico* si $S = S^{-1} = \{s^{-1} : s \in S\}$.

Definición 1.2.1. Sea G un grupo y S un subconjunto simétrico de G tal que $e \notin S$. El **grafo de Cayley** de G relativo a S, denotado por $Cay(G,S)$, es el grafo con conjunto de vértices G, tal que $\{x,y\}$ es una arista si y sólo si $xy^{-1} \in S$.

A continuación damos algunos resultados sobre las propiedades y estructura de los grafos de Cayley. Recordamos que si $\mathcal{G} = (V,E)$ es un grafo con conjunto de vértices V y de lados E, el grupo $\mathrm{Aut}(\mathcal{G})$ de automorfismos de $\mathcal{G}$ es el conjunto de permutaciones de V que preservan E.

Teorema 1.2.2. *Sea $Cay(G,S)$ el grafo de Cayley de G relativo al conjunto S. Entonces, la representación regular a derecha G_{right} de G es un subgrupo de* $\mathrm{Aut}(Cay(G,S))$.

Todos los grafos de Cayley son vértices-transitivos.

Corolario 1.2.3. *Sea $Cay(G,S)$ un grafo de Cayley con conjunto de vértices V. Dados $v,w \in V$ existe un automorfismo $f = f_{v,w} : V \to V$ tal que $f(v) = w$.*

Teorema 1.2.4. *Sea $G = \{g_1, \ldots, g_n\}$ un grupo abeliano, $S \subset G$ un subconjunto simétrico y $\chi : G \to \mathbb{C}$ un carácter de G. Sea A la matriz de adyacencia de $Cay(G,S)$ y $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ con $x_i = \chi(g_i)$. Entonces, x es un autovector de A con autovalor $\lambda = \sum_{s \in S} \chi(s)$. Más aún, todos los autovalores de A son de la forma $\sum_{s \in S} \psi(s)$, con ψ un carácter de G.*

Recordemos que un **grafo con pesos** es un par $(\mathcal{G}, w)$ donde $\mathcal{G} = (V,E)$ es un grafo no dirigido y w es una función $w : E \to S$, donde S es un conjunto, que asigna a cada arista un elemento de S. También se suele decir que $(\mathcal{G}, w)$ es un **grafo coloreado** o un **grafo con etiquetas**. Ahora definimos los grafos de Cayley con pesos.

Definición 1.2.5. Sea G un grupo y $\mathcal{P} = \{P_i\}_{i=0}^{m}$ una partición simétrica de G, es decir $P_0 = \{e\}$ y $P_i = P_i^{-1}$ para $i = 1, \ldots, m$. El **grafo de Cayley con pesos** de G relativo a $\mathcal{P}$, $Cay(G, \mathcal{P})$, es el grafo con vértices G, tal que $\{x, y\}$ es una arista de peso i si y sólo si $xy^{-1} \in P_i$.

Notar que dado un grafo de Cayley coloreado $Cay(G, \mathcal{P})$, cada $Cay(G, P_i)$ es un subgrafo. Mas aún, $Cay(G, \mathcal{P})$ es la unión de todos sus subgrafos de Cayley:

$$Cay(G, \mathcal{P}) = Cay(G, P_1) \cup \cdots \cup Cay(G, P_m). \tag{1.5}$$

1.3. Esquemas de asociación

La teoría de esquemas de asociación es de gran importancia en la combinatoria algebraica. El concepto de esquemas de asociación fue introducido por Bose y Shimamoto en [6] y la estructura algebraica correspondiente fue desarrollada por Bose y Mesner ([5]). Pero fue Delsarte quien demostró la importancia de los esquemas de asociación en el contexto de la teoría de códigos, en su monumental tesis ([14]). Más recientemente, en [15] se realiza una consideración más actual sobre el papel de los esquemas de asociación en el estudio de códigos aditivos y otros aspectos relevantes a la teoría de códigos.

Definición 1.3.1. Un **esquema de asociación de orden** n **con** s **clases** es un par $\mathcal{X} = (X, \mathcal{R})$ donde X es un conjunto finito de n elementos y $\mathcal{R} = \{R_0, R_1, \ldots, R_s\}$ es un conjunto de relaciones (clases) en X que cumplen:

(i) $R_0 = \{(x, x) : x \in X\}$ es la relación identidad.

(ii) Para cada $x, y \in X$, $(x, y) \in R_i$ para exactamente un único i, es decir

$$X \times X = R_0 \cup \cdots \cup R_s \quad \text{y} \quad R_i \cap R_j = \varnothing \text{ para todo } i \neq j.$$

(iii) $R_i^{-1} = \{(x, y) : (y, x) \in R_i\} \in \mathcal{R}$ para todo $R_i \in \mathcal{R}$.

(iv) Si $(x, y) \in R_k$, entonces la cantidad de elementos $z \in X$ tales que $(x, z) \in R_i$ y $(z, y) \in R_j$ es una constante c_{ij}^k que depende sólo de i, j, k pero no de la elección de x e y. Es decir,

$$|\{z \in X : (x, z) \in R_i \text{ y } (z, y) \in R_j\}| = c_{ij}^k.$$

Además, $\mathcal{X}$ se llama **simétrico** si cada R_i es simétrico, es decir

(v) $(x, y) \in R_i \Leftrightarrow (y, x) \in R_i$, para todo $R_i \in \mathcal{R}$.

Las constantes c_{ij}^k se llaman los **parámetros del esquema** o **constantes estructurales**. Un esquema de asociación que cumple que $c_{ij}^k = c_{ji}^k$ se dice **conmutativo**.

Notar que, en particular, si un esquema es simétrico, entonces es conmutativo.

Ejemplo 1.3.2 (Esquema de Hamming)**.** En este esquema, que se denota por $H(n,q)$, el conjunto X es el conjunto de vectores binarios de longitud n, es decir $X = \mathbb{F}_q^n$. Las relaciones están dadas por $(x,y) \in R_i$ si la distancia de Hamming entre x e y es i, es decir si

$$d_{Ham}(x,y) = |\{k \in [1,n] : x_k \neq y_k\}| = i.$$

Claramente, las condiciones (i) a (iv) de la Definición 1.3.1 se satisfacen, por lo que $H(n,q)$ resulta un esquema simétrico.

Ejemplo 1.3.3 (Grupos finitos)**.** Un grupo finito G es a su vez un esquema de asociación sobre $X = G$, con una clase $R_g = \{(x,y) : x = g*y\}$ por cada elemento $g \in G$, donde $*$ es la operación del grupo. Este esquema de asociación es conmutativo si y sólo si G es abeliano. Es decir que la noción de esquema de asociación es en cierta forma una generalización de la noción de grupo, y los esquemas simétricos generalizan los grupos abelianos.

Observación 1.3.4. A veces es útil pensar en un esquema de asociación simétrico como un grafo completo etiquetado, donde cada vértice corresponde a cada elemento de X, y la arista (x,y) tiene la etiqueta i si $(x,y) \in R_i$. Cada arista tiene una única etiqueta. Es decir un grafo completo "particionado" en los grafos básicos $\Gamma_i = (X, R_i)$.

Las relaciones también pueden describirse por sus matrices de adyacencia $A_0, A_1, \ldots, A_s$, donde A_i es la matriz de adyacencia del grafo (X, R_i). Ésta es la matriz $n \times n$, cuyas filas y columnas corresponden a los elementos de X, definida por:

$$(A_i)_{xy} = \begin{cases} 1 & \text{si } (x,y) \in R_i, \\ 0 & \text{si } (x,y) \notin R_i. \end{cases} \tag{1.6}$$

Luego, la definición de esquema de asociación es equivalente a decir que las matrices A_i son $(0,1)$-matrices (sólo con entradas 0's y 1's) de tamaño $n \times n$ que cumplen:

(i) $A_0 = I$,

(ii) $J = A_0 + A_1 + \cdots + A_s$ donde $J_{ij} = 1$ para todo $i, j = 1, \ldots, n$,

(iii) $A_i A_j = \sum_{k=0}^{s} c_{ij}^k A_k = A_j A_i$ para $i, j = 0, \ldots, s$,

En el caso en que el esquema es simétrico, además se pide que

(iv) A_i es simétrica para $i = 0, \ldots, s$.

Ahora, consideremos el espacio vectorial $\mathcal{B}$ que consiste de todas las combinaciones lineales complejas de las matrices A_i, es decir

$$\mathcal{B} = \Big\{ A = \sum_{k=0}^{s} a_k A_k : a_k \in \mathbb{C} \Big\}. \tag{1.7}$$

Por (iv), las matrices en $\mathcal{B}$ son simétricas, por (ii) las matrices $A_0, \ldots, A_s$ son linealmente independientes, y la dimensión de $\mathcal{B}$ es $s+1$. Además, por (iii), $\mathcal{B}$ es cerrado por multiplicación, operación que además es asociativa y conmutativa. Entonces $\mathcal{B}$ es un álgebra, llamada el **álgebra de Bose-Mesner** del esquema de asociación $(X, \mathcal{R})$. Es decir, es el álgebra de matrices $\mathcal{B}$ cuya base consiste en las matrices de adyacencia A_i de los grafos (X, R_i). Esta base se llama base estándar de $\mathcal{B}$.

Teorema 1.3.5. *Sea $\mathcal{X} = (X, \{R_i\}_{0 \le i \le s})$ un esquema de asociación conmutativo de clase s y orden n, con matrices de adyacencia $\{A_i\}$. Entonces existe una descomposición de $\mathbb{C}^n$ como suma directa de autoespacios maximales comunes de las matrices de adyacencia, dada por $\mathbb{C}^n = V_0 \oplus V_1 \oplus \cdots \oplus V_r$, para algún r. Sea E_i la matriz de la proyección ortogonal de $\mathbb{C}^n$ en V_i con respecto a la base canónica de $\mathbb{C}^n$. Entonces, cada E_i es una combinación lineal de $A_0, A_1, \ldots, A_s$. En particular, $r = s$ y E_i son los idempotentes del álgebra de Bose-Mesner de $\mathcal{X}$.*

Sea $\mathcal{X}$ un esquema de asociación de clase d y orden n. Por el teorema anterior tenemos

$$A_i = \sum_{j=0}^{d} p_i(j) E_i, \qquad\qquad E_i = \tfrac{1}{n} \sum_{j=0}^{d} q_i(j) A_j. \tag{1.8}$$

La matriz P que representa el cambio de base de las matrices de adyacencia $A_0, A_1, \ldots, A_d$ a la base de idempotentes $E_0, E_1, \ldots, E_d$, es decir $P_{ji} = p_i(j)$, se denomina la **primera automatriz** de $\mathcal{X}$. La matriz Q definida por $Q_{ji} = q_i(j)$ se denomina la **segunda automatriz**. Claramente tenemos que $PQ = QP = nI_{d+1}$, donde I_{d+1} denota la matriz identidad de dimensión $d+1$.

Definición 1.3.6. Sea $\mathcal{X}$ un esquema de asociación de clase d y orden n. El **grupo de automorfismos** de $\mathcal{X}$, que denotaremos por $\mathbf{Aut}(\mathcal{X})$, se define como la intersección de todos los automorfismos de sus grafos básicos:

$$\mathbf{Aut}(\mathcal{X}) = \bigcap_{i=0}^{s} \mathbf{Aut}(X, R_i),$$

donde $\mathbf{Aut}(X, R_i)$ es el automorfismo del grafo (X, R_i).

Definición 1.3.7. Un esquema de asociación $\mathcal{X} = (X, \mathcal{R} = \{R_0, \ldots, R_s\})$ tal que $G_{right} \le \mathbf{Aut}(\mathcal{X})$ se dice **esquema de asociación de Cayley** sobre G. También suelen llamarse **esquemas de traslación**, generalmente en el caso que G sea abeliano.

A continuación daremos algunos ejemplos de grupos de automorfismos de grafos computables.

Para ello, primero necesitaremos recordar las definiciones de producto corona de grupos de permutación y composición de grafos.

Definición 1.3.8. Un **grupo de permutaciones** es un grupo cuyos elementos son permutaciones de un conjunto X, y cuya operación es la composición de permutaciones de X, al cual denotaremos (G,X). El conjunto de todas las permutaciones de X, es el **grupo simétrico** de X y se denota $\mathbb{S}_X$. Entonces un grupo de permutaciones es un subgrupo del grupo simétrico, i.e. $G \subseteq \mathbb{S}_X$.

Sean (G,X) y (H,Y) grupos de permutación. El producto $G^Y = Map(Y,G) = \{f : Y \to G\}$ actúa sobre $X \times Y$, en las primeras coordenadas de la siguiente forma,

$$f(x,y) = (f(y)x,y) \qquad x \in X, y \in Y, f \in Map(Y,G).$$

Por otra parte, el grupo H actúa sobre $X \times Y$, en la segunda coordenada.

$$h(x,y) = (x,h(y)) \qquad x \in X, y \in Y, h \in H.$$

Además H actúa en G^Y permutando coordenadas:

$$(hf)(y) = f(h^{-1}(y)).$$

Por lo tanto, el producto semidirecto $G^Y \rtimes H$ actúa en $X \times Y$. Este grupo de permutación se denomina el **producto corona** de (G,X) y (H,Y) y se denota $G \wr H$.

Definición 1.3.9. La **composición** $\mathcal{G} = \mathcal{G}_1[\mathcal{G}_2]$ de grafos $\mathcal{G}_1$ y $\mathcal{G}_2$ (también denominado **producto lexicográfico**) con conjuntos de vértices disjuntos X_1 y X_2, y conjuntos de aristas E_1 y E_2, es el grafo, cuyos vértices son $X_1 \times X_2$ y $x = (x_1,x_2)$ es adyacente a $y = (y_1,y_2)$ si se cumple alguna de las siguientes condiciones:

(i) x_1 es adyacente a y_1,

(ii) $x_1 = y_1$ y x_2 es adyacente a y_2.

Observación 1.3.10. Los siguientes son grupos de automorfismos de grafos conocidos (para los primeros tres casos ver [8] y para el último, ver [19]).

- $\mathrm{Aut}(\mathcal{G}) = \mathrm{Aut}(\mathcal{G}^c)$, donde $\mathcal{G}^c$ es el grafo complementario de $\mathcal{G}$.
- $\mathrm{Aut}(K_n) = \mathbb{S}_n$.
- $\mathrm{Aut}(n\mathcal{G}) = \mathrm{Aut}(\mathcal{G}) \wr \mathbb{S}_n$, donde $n\mathcal{G}$ es la unión disjunta de n copias de $\mathcal{G}$.
- $\mathrm{Aut}(\mathcal{G}[K_n^c] = \mathrm{Aut}(K_n^c) \wr \mathrm{Aut}(\mathcal{G})$, donde $\mathcal{G}[K_n^c]$ es la *composición* (también llamado producto lexicográfico) de los grafos $\mathcal{G}$ y $\mathcal{H}$.

1.4. Álgebras de grupo

Definición 1.4.1. Dado un grupo finito G y un cuerpo $\mathbb{F}$, el **álgebra de grupo** $\mathbb{F}[G]$ se define como el espacio vectorial de sumas formales

$$\mathbb{F}[G] = \Big\{ \sum_{g\in G} a_g g \ : \ a_g \in \mathbb{K} \Big\}$$

con las operaciones

$$\Big(\sum_{g\in G} a_g g\Big) + \Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G} (a_g + b_g) g \qquad \text{y} \qquad a\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} (a a_g) g, \quad a \in \mathbb{F},$$

donde el producto en $\mathbb{F}[G]$ resulta de extender por linealidad el producto de G

$$\Big(\sum_{g\in G} a_g g\Big)\Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G, h\in G} (a_g b_h) gh.$$

Definición 1.4.2. Sea $\mathcal{A}$ un álgebra.

(i) Un elemento $e \in \mathcal{A}$ es un **idempotente** si $e^2 = e$.

(ii) Dos idempotentes e_1 y e_2 son **ortogonales** si $e_1 e_2 = e_2 e_1 = 0$.

(iii) Un idempotente e se dice **primitivo** si e no puede ser escrito de la forma $e = e_1 + e_2$, donde e_1 y e_2 son idempotentes ortogonales.

(iv) J se dice un **idempotente primitivo central** si J pertenece al centro de $\mathcal{A}$, J es un idempotente, y J no puede escribirse de la forma $J = I_1 + I_2$ donde I_1 y I_2 son idempotentes ortogonales centrales.

De ahora en adelante sólo usaremos el álgebra de grupo sobre los complejos $\mathbb{C}[G]$. Primero mostraremos que el centro, $Z(\mathbb{C}[G])$, consiste de elementos diagonalizables, y luego obtendremos los idempotentes primitivos centrales de $\mathbb{C}[G]$ como la base de autovectores simultáneos del centro.

Notación: para $x \in \mathbb{C}[G]$, $\bar{x}$ denotará la conjugación compleja de x, y $x^\dagger$ el conjugado transpuesto de x, donde x es considerado como un operador lineal sobre $\mathbb{C}[G]$ por multiplicación a izquierda.

Proposición 1.4.3. *Todo elemento de $Z(\mathbb{C}[G])$ es diagonalizable (actuando por multiplicación a izquierda en $Z(\mathbb{C}[G])$).*

Demostración. Como operador en $\mathbb{C}[G]$ por multiplicación a izquierda, cada elemento g es una matriz de permutación, y por lo tanto $g^\dagger = g^{-1}$. Entonces, para todo $x = \sum_{g\in G} c_g g \in \mathbb{C}[G]$, se tiene que $x^\dagger = \sum_{g\in G} \bar{c}_g g^{-1} \in \mathbb{C}[G]$. Si $z \in Z(\mathbb{C}[G])$, $zz^\dagger = z^\dagger z$, y en consecuencia, z es diagonalizable en $\mathbb{C}[G]$. Ahora la proposición sigue del hecho de que $Z(\mathbb{C}[G])$ es un subespacio invariante para z. □

Observación 1.4.4. Si $z \in Z(\mathbb{C}[G])$, entonces se tiene que $z^\dagger \in Z(\mathbb{C}[G])$. En particular, los elementos $\Omega_g = \sum_{x\in K_g} x$, de la base canónica de $Z(\mathbb{C}[G])$, donde K_g denota la clase de conjugación de g, satisfacen $\Omega_g^\dagger = \Omega_{g^{-1}}$.

Por la Proposición 1.4.3, cualquier base de $Z(\mathbb{C}[G])$ es un conjunto conmutativo de operadores diagonalizables en $Z(\mathbb{C}[G])$ –actuando por multiplicación a izquierda– y por lo tanto existe una base de autovectores de $Z(\mathbb{C}[G])$.

Teorema 1.4.5. *Existe una única base de diagonalización simultánea* $\{J_p : 1 \leq p \leq k\}$ *de* $Z(\mathbb{C}[G])$ *tal que:*

(i) $J_p^2 = J_p$,

(ii) $J_p J_q = 0$ *para* $p \neq q$,

(iii) $J_1 + \cdots + J_p = e_G$,

(iv) J_p *es un idempotente central primitivo.*

Observación 1.4.6. Dado que J_p es central, $A_p = (\mathbb{C}[G])J_p$ es un ideal bilátero de $\mathbb{C}[G]$. Por el Teorema 1.4.5, se tiene que el álgebra de grupo $\mathbb{C}[G]$ es una suma directa de ideales biláteros $\{A_p\}$,

$$\mathbb{C}[G] = \bigoplus_{p=1}^{k} A_p.$$

Observación 1.4.7. Para cada p, J_p genera el centro 1-dimensional A_p. En efecto, si $a \in Z(A_p)$, entonces se tiene que $a \in Z(\mathbb{C}[G])$, y por lo tanto, $a = aJ_p = \lambda J_p$, para algún λ, donde la primera igualdad sigue de que $a \in A_p$ y la segunda igualdad vale porque J_p es un autovector de $a \in Z(\mathbb{C}[G])$. De esto se sigue de la observación anterior que A_p no puede descomponerse como suma directa de ideales biláteros.

Es bien sabido que los bloques A_p son simples, y por lo tanto isomorfos a un álgebra de matrices.

A continuación veremos varias ilustraciones del Teorema 1.4.5, o sea, de que los idempotentes centrales primitivos forman una base de diagonalización simultánea de $Z(\mathbb{C}[G])$.

Proposición 1.4.8. *Un grupo finito* G *es abeliano si y sólo si* $\mathbb{C}[G] \simeq \mathbb{C}^k$.

Demostración. Si G es abeliano, entonces $\mathbb{C}[G]$ es un álgebra conmutativa. Sea $\{J_p\}$ la base de diagonalización simultánea de $\mathbb{C}[G]$, como en el Teorema 1.4.5. Entonces, para todo $g \in G$, $gJ_p = \lambda_p(g)J_p$ donde $\lambda_p(g) \in \mathbb{C}$. Por lo tanto, $\mathbb{C}[G] = \bigoplus_{p=1}^{k} \mathbb{C}J_p \simeq \mathbb{C}^k$. La recíproca es trivial. □

Ahora, describimos la base de autovectores simultáneos para un grupo cíclico de orden k.

Proposición 1.4.9. *Sea* $G = \langle r \rangle$ *un grupo cíclico de orden* k *y* $\omega = \exp(2\pi i/k)$ *la raíz primitiva* k*-ésima de la unidad. Los idempotentes ortogonales*

$$J_p = \tfrac{1}{k} \sum_{m=1}^{k} \omega^{-mp} r^m, \qquad 1 \leq p \leq k,$$

forman la base de diagonalización simultánea de $\mathbb{C}[G]$.

Demostración. Como el polinomio minimal de r es $x^k - 1$, los distintos autovalores de r son $\lambda_p = \omega^p$, $1 \leq p \leq k$. Sea $v = \sum_{m=1}^{k} a_m r^m$ un autovector de r correspondiente al autovalor λ. Entonces $rv = \lambda v$ implica que

$$a_k = \lambda a_1 = \lambda^2 a_2 = \cdots = \lambda^{k-1} a_{k-1}.$$

Tomando $a_k = 1$, los autovectores de r con autovalor $\lambda_p = \omega^p$ son múltiplos de $v_p = \sum_{m=1}^{k} \omega^{-mp} r^m$. Ahora,

$$v_p v_q = \sum_{m=1}^{k} \omega^{-mp} r^m v_q = \sum_{m=1}^{k} \omega^{-m(p-q)} v_q = \begin{cases} 0 & \text{si} \quad q \neq p, \\ k v_q & \text{si} \quad q = p. \end{cases}$$

Por lo tanto, los idempotentes (ortogonales) son $J_p = \frac{1}{k} v_p$. □

Para el álgebra de grupo de un grupo abeliano finito, la base de diagonalización simultánea del Teorema 1.4.5 se obtiene utilizando la Proposición 1.4.9, junto con el siguiente resultado:

Proposición 1.4.10. *Sean G_i grupos finitos, entonces se tiene que*

$$\mathbb{C}[G_1 \times G_2 \times \cdots \times G_n] \simeq \mathbb{C}[G_1] \otimes \mathbb{C}[G_2] \otimes \cdots \otimes \mathbb{C}[G_n].$$

Demostración. El isomorfismo está dado por $\phi(g_1, g_2, ..., g_n) = g_1 \otimes g_2 \otimes \cdots \otimes g_n$ luego de extenderlo linealmente. □

Para un grupo abeliano finito $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, donde $\mathbb{Z}_{n_i}$ es el grupo cíclico de orden n_i, la base de autovectores idempotentes para cada $\mathbb{C}[\mathbb{Z}_{n_i}]$ está dada por la Proposición 1.4.9. Sean $J_p^{(i)}$, $1 \leq p \leq n_i$ los idempotentes para cada $\mathbb{Z}_{n_i}$. Entonces la base de autovectores idempotentes de $\mathbb{C}[G]$ está dada por

$$J_{p_1}^{(1)} J_{p_2}^{(2)} \cdots J_{p_k}^{(k)}$$

donde $1 \leq p_i \leq n_i$ para cada i.

Observación 1.4.11. Para un grupo abeliano G, los idempotentes primitivos centrales de $\mathbb{C}[G]$ son idempotentes primitivos. Cuando G es no abeliano, $Z(\mathbb{C}[G])$ es una subálgebra propia de $\mathbb{C}[G]$. En este caso, cada idempotente central primitivo se descompone como una suma de idempotentes primitivos ortogonales,

$$J_p = u_1^p + u_2^p + \cdots + u_{n_p}^p.$$

1.5. Anillos de Schur

Los anillos de Schur fueron estudiados originalmente por Schur y Wielandt a principios del siglo XX, para el estudio de grupos de permutaciones, pero en las últimas décadas han surgido aplicaciones en combinatoria, teoría de grafos y teoría de diseños ([28, 36]). En esta sección daremos los conceptos básicos sobre anillos de Schur, formas de construirlos y algunos resultados sobre su clasificación. Para una información mas detallada del tema recomendamos leer [43] y [39].

Si $\mathcal{P} = \{P_0, \ldots, P_m\}$ es una partición de un conjunto X, es decir $X = P_0 \cup \cdots \cup P_m$ con $P_i \cap P_j = \varnothing$ para todo $i \neq j$, usaremos la notación

$$\mathcal{P} = \mathcal{P}(X) = P_0 \mid \cdots \mid P_m.$$

Definición 1.5.1. Sea $C \subseteq G$, definimos

$$\overline{C} = \sum_{c \in C} c \in \mathbb{C}[G]. \tag{1.9}$$

Un elemento $\alpha \in \mathbb{C}[G]$ es un **elemento simple** si $\alpha = \overline{C}$ para algún $C \subseteq G$. Si $C = \emptyset$, entonces $\overline{C} = 0$.

Definición 1.5.2. Un anillo $\mathcal{A} \subseteq \mathbb{C}[G]$ se dice **anillo de Schur** (o S**-anillo**), sobre el grupo G si existe una partición $\mathcal{P} = \mathcal{P}_{\mathcal{A}}(G) = P_0 | \cdots | P_d$ de G que satisface las siguientes condiciones:

(i) $\{e\} \in \mathcal{P}$.

(ii) El conjunto $\overline{\mathcal{P}} = \{\overline{P_0}, \overline{P_1}, \ldots, \overline{P_d}\}$ es una base de $\mathcal{A}$ como espacio vectorial.

(iii) $P^{-1} \in \mathcal{P}$, para todo $P \in \mathcal{P}$.

Además, $\mathcal{A}$ se llama **simétrico** si cada P_i es simétrico, es decir:

(iv) $P_i^{-1} = P_i$ para $i = 0, \ldots, d$.

Una partición $\mathcal{P}$ de G se dice **partición de Schur** si $\mathcal{P}$ satisface las condiciones (i) y (iii), y además $\mathcal{A} = \langle \overline{\mathcal{P}} \rangle$ es una subálgebra de $\mathbb{C}[G]$. La **dimensión** de $\mathcal{A}$ es su dimensión como espacio vectorial.

Se puede ver que existe la siguiente correspondencia 1 – 1 entre anillos y particiones de Schur

$$\{\text{anillos de Schur de } G\} \longleftrightarrow \{\text{particiones de Schur de } G\}.$$

Sea S sea un anillo de Schur sobre el grupo finito G dado por la partición $\{P_1, P_2, \ldots, P_d\}$. Los subconjuntos $P_1, \ldots, P_d$ se denominan **conjuntos primitivos** de S o S**-clases**. Denotamos por $\mathcal{D}(S)$ al conjunto de S-clases, es decir

$$\mathcal{D}(S) = \{P_1, \ldots, P_d\}.$$

Si $C \subseteq G$ y $\overline{C} \in S$, entonces C se dice que es un S**-conjunto**. Si C también es un subgrupo de G, diremos que C es un S**-subgrupo** de G.

Ejemplo 1.5.3. Sea S un anillo de Schur sobre G. Si H es un S-subgrupo de G, entonces

$$S_H := \mathrm{Span}_F\{\overline{C_i} : C_i \subseteq H\}. \tag{1.10}$$

es un anillo de Schur de H.

Una caracterización de los anillos de Schur

Definimos dos operaciones adicionales en $\mathbb{F}[G]$ naturales: la operación estrella

$$* : \mathbb{F}[G] \to \mathbb{F}[G] : \quad \Big(\sum_{g\in G} \alpha_g g\Big)^* = \sum_{g\in G} \alpha_g g^{-1}$$

y el **producto de Hadamard**

$$\circ : \mathbb{F}[G] \times \mathbb{F}[G] \to \mathbb{F}[G] : \quad \Big(\sum_{g\in G} \alpha_g g\Big) \circ \Big(\sum_{g\in G} \beta_g g\Big) = \sum_{g\in G} \alpha_g \beta_g g.$$

Los anillos de Schur pueden ser caracterizados por estas operaciones. Por ejemplo, los subespacios de $\mathbb{F}[G]$ cerrados por $\circ$ son exactamente aquellos generados por los elementos simples.

Proposición 1.5.4 ([41], Lemma 1.3)**.** *Sea S una subálgebra de $\mathbb{F}[G]$. Entonces S es un anillo de Schur si y sólo si S es cerrada por las operaciones $*$ y $\circ$ y además $1 \in S$, $\overline{G} \in S$.*

Corolario 1.5.5. *Si S y T son anillos de Schur sobre G entonces $S \cap T$ es un anillo de Schur sobre G.*

Ejemplo 1.5.6.

(i) Sea G un grupo y sean $P_0 = \{e\}$ y $P_1 = G \setminus \{e\}$, entonces $\mathcal{P} = \{P_0, P_1\}$ es una partición de Schur, más aún, $\mathcal{A} = \langle \overline{\mathcal{P}} \rangle$ es el único S-anillo de dimensión 2 sobre G y se denomina **anillo de Schur trivial** denotado $\mathbb{F}[G]^0$.

(ii) Toda álgebra de grupo $\mathbb{F}[G]$ es un anillo de Schur, generado por la partición $\mathcal{P} = \{g\}_{g\in G}$.

Algunas construcciones y productos de anillos de Schur

A continuación veremos algunas de las construcciones de anillos de Schur mas importantes, asi como operaciones entre anillos de Schur que nos permiten obtener nuevos anillos en función de otros.

Anillos de Schur orbitales

Sea $\mathcal{H} \leq Aut(G)$ y

$$\mathbb{C}[G]^{\mathcal{H}} = \{\alpha \in \mathbb{C}[G] \ : \ \sigma(\alpha) = \alpha \ \forall \sigma \in \mathcal{H}\}. \tag{1.11}$$

Entonces $\mathbb{C}[G]^{\mathcal{H}}$ es un anillo de Schur generado por la partición de G correspondiente a la acción de $\mathcal{H}$ en G. Estos anillos se denominan **anillos de Schur orbitales** y su conjunto de S-clases $\mathcal{D}(\mathbb{C}[G]^{\mathcal{H}})$ consiste en las $\mathcal{H}$-órbitas de G. Notar que el centro de $\mathbb{C}[G]^{\mathcal{H}}$ es un anillo orbital con $\mathcal{H} = Inn(G)$, donde $Inn(G)$ denota el grupo de automorfismos interiores de G .

Anillos de Schur racionales

Consideremos el siguiente anillo de Schur

$$\mathcal{R}(\mathbb{C}[G]) = \mathbb{C}[G]^{Aut(G)}$$

cuyos conjuntos primitivos son las clases de automorfismos de G. Todo anillo contenido en $\mathcal{R}(\mathbb{C}[G])$ se denomina **anillo de Schur racional** ya que es fijado por el grupo de automorfismos de G.

Anillos de Schur simétricos

Si G es abeliano, consideremos el siguiente anillo de Schur sobre G

$$\mathcal{S}(\mathbb{C}[G]) = \mathbb{C}[G]^{\langle * \rangle}$$

donde $\langle * \rangle \leq Aut(G)$, y $*$ es el automorfismo de inversión $g^* = g^{-1}$, y cuyos conjuntos primitivos son las clases inversas de G. Todo elemento $\alpha \in \mathbb{C}[G]$ se dice **simétrico** si $\alpha^* = \alpha$, por lo tanto $\mathcal{S}(\mathbb{C}[G])$ es el conjunto de todos los elementos simétricos de $\mathbb{C}[G]$. Se denomina **anillo de Schur simétrico** a todo anillo de Schur contenido en $\mathcal{S}(\mathbb{C}[G])$.

Producto directo de anillos de Schur

Sean S y T anillos de Schur sobre G y H, respectivamente. Podemos pensar a G y H naturalmente como subgrupos de $G \times H$. Definimos el **producto punto** de S y T como:

$$S \cdot T = Span\{\overline{C} \cdot \overline{D} \ : \ C \in \mathcal{D}(S), D \in \mathcal{D}(T)\},$$

donde $\overline{C} \cdot \overline{D}$ es el producto en el álgebra $\mathbb{C}[G \times H]$, y el cual es un anillo de Schur con la partición

$$\mathcal{D}(S \cdot T) = \{C \times D \subseteq G \times H \ C \in \mathcal{D}(S), D \in \mathcal{D}(T)\},$$

por esta razón también suele denominarse **producto directo** de S y T, denotado $S \times T$. Mas aún, $S \cdot T \simeq S \otimes_F T$, como F-álgebras. Debido a esto, el anillo de Schur $S \cdot T$ algunas veces es llamado **producto tensorial** de anillos de S y T, denotado $S \otimes T$.

Producto corona de anillos de Schur

Sean $H \trianglelefteq G$, S un anillo de Schur sobre G/H y $\pi : G \to G/H$ el mapa cociente canónico. Consideremos la partición de G dada por

$$\mathcal{D}(\pi^{-1}(S)) = \{\pi^{-1}(C) : C \in \mathcal{D}(S)\},$$

es decir, si $C = \{g_1H, g_2H, \ldots, g_kH\} \in \mathcal{D}(S)$, entonces $\pi^{-1}(C) = \bigcup_{i=1}^{k} g_iH \in \mathcal{D}$. Sea

$$\pi^{-1}(S) = \mathrm{Span}_F\{\overline{D} : D \in \mathcal{D}\}.$$

Luego, $\pi^{-1}(S)$ es una subálgebra de $\mathbb{F}[G]$ cerrada por las operaciones $*$ y $\circ$ y contiene a $\overline{H}$ y $\overline{G}$, denominado el **anillo de Schur extendido** de S sobre G.

Sea $H \trianglelefteq G$, y sean S y T anillos de Schur sobre H y G/H, respectivamente. El **producto corona** (wreath) de S y T es

$$S \wr T = S + \pi^{-1}(T).$$

El producto corona $S \wr T$ es también un anillo de Schur con partición

$$\mathcal{D}(S \wr T) = \mathcal{D}(S) \cup (\mathcal{D}(\pi^{-1}(T)) \setminus \{H\}).$$

Se sigue que

$$(S \wr T)_H = S \quad \text{y} \quad \pi(S \wr T) = T$$

con la notación de (1.10).

Producto cuña de anillos de Schur

Sea $1 < K \leq H < G$ una secuencia de grupos finitos tales que $K \trianglelefteq G$. Sea S un anillo de Schur sobre H y T un anillo de Schur sobre G/K. Sea $\pi : G \to G/K$ el mapa cociente. Sea

$$S \wedge_K T = S + \pi^{-1}(T)$$

el **producto cuña** (wedge) de S y T. Cuando el contexto sea claro, el subíndice puede ser omitido. Si asumimos que H/K es un T-subgrupo, K es un S-subgrupo, y $\pi(S) = T_{H/K}$, entonces $S \wedge T$ es un anillo de Schur sobre G con partición

$$\mathcal{D}(S \wedge T) = \mathcal{D}(S) \cup (\mathcal{D}(\pi^{-1}(T)) \setminus \mathcal{D}(\pi^{-1}(T_{H/K}))). \tag{1.12}$$

Como en el caso anterior, se tiene que

$$(S \wedge T)_H = S \quad \text{y} \quad \pi(S \wedge T) = T.$$

Si $H = K$, entonces $S \wedge T = S \wr T$. Por lo tanto, el producto cuña de anillos de Schur es un producto corona generalizado.

Sea S un anillo de Schur sobre G. Si existen subgrupos $1 < K \leq H < G$, con $K \trianglelefteq G$, y anillos de Schur R y T sobre H y G/K, respectivamente, tales que $S = R \wedge_K T$, entonces diremos que S es *cuña-descomponible*; de otra forma, diremos que S es *cuña-indescomponible*. Si S es cuña-descomponible, llamaremos a $1 < K \leq H < G$ una *cuña-descomposición* de S. Definimos los términos *corona-descomponible*, *corona-indescomponible* y *descomposición corona* análogamente.

Anillos de Schur reticulares

Sea G un grupo finito, y sea $\mathcal{L}$ un retículo de subgrupos normales de G. Entonces definimos:

$$S(\mathcal{L}) = Span\{\overline{H} \ : \ H \in \mathcal{L}\} \in \mathbb{C}[G].$$

Como $\overline{H} \circ \overline{K} = \overline{H \cap K} \in S(\mathcal{L})$ y $\overline{H} \cdot \overline{K} = |H \cap K| \, \overline{HK} \in S(\mathcal{L})$, para todo $H, K \in S(\mathcal{L})$, se tiene que $S(\mathcal{L})$ es un anillo de Schur que llamaremos **anillo de Schur reticular**.

Ejemplo 1.5.7. Sea G un grupo finito, supongamos que tenemos una cadena de subgrupos normales

$$1 < G_1 < G_2 < \cdots < G_n < G,$$

entonces el anillo reticular inducido, esta dado por la partición

$$G_1 \setminus 1, \ G_2 \setminus G_1, \ \ldots, \ G \setminus G_n.$$

Anillos de Schur sobre $\mathbb{Z}_n$

Leung y Man en [30, 31] usaron estas construcciones mencionadas anteriormente para clasificar todos los anillos de Schur sobre $\mathbb{Z}_n$.

Teorema 1.5.8 ([30, 31])**.** *Sea S un anillo de Schur sobre $G = \mathbb{Z}_n$. Entonces S es trivial, orbital, producto directo, producto corona o producto cuña de anillos de Schur.*

Corolario 1.5.9. *Sea S un anillo de Schur sobre $G = \mathbb{Z}_{p^n}$ con p primo. Entonces S es trivial, orbital o un producto cuña de anillos de Schur.*

Demostración. Como G es un p-grupo cíclico, no puede ser expresado como un producto directo no trivial de grupos. Por lo tanto, S no puede ser expresado como un producto directo no trivial de anillos de Schur. El resultado sigue de Teorema 1.5.8. □

Corolario 1.5.10. *Sea S un anillo de Schur sobre Sea $G = \mathbb{Z}_p$ con p primo. Entonces S es un anillo de Schur orbital.*

Demostración. Dado que G no tiene subgrupos no triviales, S es cuña-indescomponible. Además, $\mathbb{F}[G]^0 = \mathcal{R}(\mathbb{F}[G])$. Por lo tanto, el resultado sigue de Corolario 1.5.9. □

Corolario 1.5.11. *Sea $G = \mathbb{Z}_{p^n}$ con p primo. Entonces, para cualquier anillo de Schur S que es cuña-descomponible sobre G, existe una cuña-descomposición $1 < K \leq H < G$ tal que S_H es un anillo orbital cuña-indescomponible o es el anillo de Schur trivial sobre H.*

Demostración. Por hipótesis, S tiene una cuña-descomposición $1 < K \leq H < G$. Si S_H es cuña-descomponible, entonces también tiene una cuña descomposición $1 < K' \leq H' < H$. Dado que K y K' son subgrupos no triviales de $\mathbb{Z}_{p^n}$, $K \cap K'$ también es no trivial. Toda S-clase fuera de H es una unión de coclases de K. Por lo tanto tal S-clase es también una unión de coclases de $K \cap K'$. Similarmente, toda S-clase adentro de H pero afuera de H' es una unión de coclases de $K \cap K'$. Por lo tanto, $1 < K \cap K' \leq H' < G$ es una cuña-descomposición de S. Se sigue que una cuña-descomposición $1 < K \leq H < G$ de S se puede elegir tal que H sea minimal. Tal elección implica que S_H debe ser cuña-indescomponible. Por Corolario 1.5.9, S_H es un anillo de Schur orbital o el anillo trivial. □

En general no hay una clasificación de anillos de Schur en el caso que G no sea cíclico, de hecho existen anillos de Schur que no son del tipo mencionado en el Teorema 1.5.8.

Isomorfismos

A continuación definimos algunas nociones de equivalencia entre anillos de Schur.

- Dos anillos de Schur S y T, sobre H y K respectivamente, se dicen **algebraicamente isomorfos**, notación $S \simeq_{alg} T$, si existe una biyección $\phi : \mathcal{D}(S) \to \mathcal{D}(T)$ tal que el mapa $P \mapsto \phi(P)$ induce un isomorfismo entre las álgebras S y T.
- Dos anillos de Schur $S =< \overline{P_0}, \ldots, \overline{P_s} > \subseteq \mathbb{C}[H]$ y $T =< \overline{Q_0}, \ldots, \overline{Q_r} > \subseteq \mathbb{C}[K]$ se dicen **combinatoriamente isomorfos**, notación $S \simeq_{com} T$, si $s = r$ y existe una biyección $f : H \to K$ tal que f es un isomorfismo de los esquemas de Cayley $Cay(H,S)$ y $Cay(K,T)$.
- Dos anillos de Schur S y T, sobre H y K respectivamente, se dicen **Cayley isomorfos**, notación $S \simeq_{Cay} T$, si existe un isomorfismo de grupos $\varphi : H \to K$ tal que el isomorfismo $\mathbb{C}[G] \to \mathbb{C}[G]$ inducido por φ, es una biyección entre S y T.

Se tiene la siguiente relación entre estos distintos tipos de isomorfismos

$$S \simeq_{Cay} T \implies S \simeq_{com} T \implies S \simeq_{alg} T. \tag{1.13}$$

Dualidad

Sea G un grupo abeliano, y sea $\widehat{G}$ el grupo de caracteres de G . Para todo anillo de Schur S sobre G, podemos definir el **anillo de Schur dual** $\widehat{S}$ sobre $\widehat{G}$ de la siguiente forma: dado $\chi \in \widehat{G}$ y $X \subset G$, definimos

$$\chi(X) = \sum_{x \in X} \chi(x). \tag{1.14}$$

Sea S un anillo de Schur sobre G, y sea $\mathcal{P}$ la partición de Schur asociada. Denotemos por $\widehat{\mathcal{P}}$ al conjunto de relaciones en $\widehat{G}$ definidas por

$$\chi_1 \sim \chi_2 \Longleftrightarrow \chi_1(X) = \chi_2(X), \quad X \in \mathcal{D}(S), \tag{1.15}$$

es decir, dos caracteres de G pertenecen a la misma S-clase de $\widehat{G}$ si tienen el mismo valor en cada uno de las S-clases del anillo S. Se tiene que $\widehat{\mathcal{P}}$ es una partición de Schur de $\widehat{G}$. El anillo de Schur $\widehat{S}$ asociado con esta partición se dice **anillo de Schur dual** de S. Se puede probar que

$$rank(S) = rank(\widehat{S}),$$

o sea que $|\mathcal{P}| = |\widehat{\mathcal{P}}|$. Además, el anillo de Schur dual a $\widehat{S}$ es S.

Se puede ver que el mapa de $Aut(G)$ en $Aut(\widehat{G})$ que lleva σ en $\widehat{\sigma}$ definido por

$$\chi^{\widehat{\sigma}}(g) = \chi(g^{\sigma}),$$

es un isomorfismo de grupos. La imagen de $K \leq Aut(G)$ bajo este isomorfismo se denota $\widehat{K}$.

Es sabido que existe un único anti-isomorfismo de retículos entre el retículos de subgrupos de G y los subgrupos de $\widehat{G}$ [60]. La imagen de un grupo $H \leq G$ con respecto a este anti-isomorfismo se denota $H^{\perp}$.

El siguiente resultado que puede encontrarse en [54, Lema 2.5], resume algunos de los hechos conocidos sobre dualidad de anillos de Schur. Para mas información sobre dualidad de Anillos de Schur puede verse [17] y [18].

Lema 1.5.12. *Sea S un anillo de Schur sobre un grupo abeliano G, entonces*

(i) S es cíclico asociado al grupo $K \leq Aut(G)$ si y sólo si $\widehat{S}$ es cíclico con $\widehat{K}$,

(ii) $S = S_1 \times S_2$ si y sólo si $\widehat{S} = \widehat{S_1} \times \widehat{S_2}$,

(iii) $S = S_1 \wr_K S_2$ si y sólo si $\widehat{S} = \widehat{S_2} \wr_{K^{\perp}} \widehat{S_1}$.

Relación con grupos de permutación

Consideremos un grupo arbitrario $H \leq \mathbb{S}_G$ que contiene a la representación regular G_{right} como subgrupo. Sean $P_0 = \{e\}, P_1, \ldots, P_s$ las órbitas de G_e, entonces el espacio vectorial generado por $\{\overline{P_i}\}_{i=0}^{s}$ es el **módulo de transitividad** de H y se denota $\mathcal{S}(G, H_e)$. El siguiente resultado fue probado por Schur.

Teorema 1.5.13. *El módulo de transitividad $\mathcal{S}(G, H_e)$ es un anillo de Schur sobre G.*

En general, no todo los anillos de Schur son el módulo de transitividad de algún grupo de permutación.

Definición 1.5.14. Un anillo de Schur sobre G, que es el módulo de transitividad de un grupo H, $G_{right} \leq H \leq \mathbb{S}_G$, se llama **schuriano**. Si todo S-anillo sobre G es schuriano, se dice que G es un **grupo de Schur**.

Teorema 1.5.15 ([16, Teo. 1.1])**.** *Es sabido que $\mathbb{Z}_n$ es un grupo de Schur si y sólo si n es de la siguiente forma*

$$p^k, \quad p^k q, \quad 2p^k q, \quad pqr, \quad 2pqr,$$

donde p, q, r son primos distintos y $k \geq 0$.

Notar que no es necesario que $2 \neq p, q, r$, por ejemplo $4p^k$ también es un grupo schuriano.

Corolario 1.5.16. *El menor número tal que $\mathbb{Z}_n$ no es un grupo de Schur es $n = 72$.*

La relación entre grupos de permutación y anillos de Schur se puede ver en el siguiente teorema que describe una correspondecia de Galois entre los anillos de Schur sobre un grupo G y los supergrupos de G_{right} en $\mathbb{S}_G$.

Teorema 1.5.17 ([28, Teo. 3.13])**.** *Sean S y T anillos de Schur sobre G, y sean H, K supergrupos de G_{right} en $\mathbb{S}_G$, entonces:*

(i) $S \subseteq T \Rightarrow \mathbf{Aut}(S) \geq \mathbf{Aut}(T)$,

(ii) $H \leq K \Rightarrow \mathcal{S}(G, H_e) \supseteq \mathcal{S}(G, K_e)$,

(iii) $S \subseteq \mathcal{S}(G, \mathbf{Aut}(S)_e)$,

(iv) $H \leq \mathbf{Aut}(\mathcal{S}(G, H_e))$.

Corolario 1.5.18. *Un anillo de Schur S sobre G es Schuriano si y sólo si $S = \mathcal{S}(G, \mathbf{Aut}(S)_e)$.*

Relación con esquemas de asociación

Originalmente los S-anillos fueron pensados por Schur como una forma de estudiar grupos de permutación, mucho tiempo después se descubrió que pueden considerarse como una caso especial de esquemas de asociación. Todo anillo de Schur $S = \langle\{\overline{P_0}, \ldots, \overline{P_s}\}\rangle$ sobre un grupo G induce un esquema de asociación sobre G cuyas relaciones básicas son los grafos de Cayley $Cay(G, P_i)$, $i \in \{0, 1, \ldots, s\}$, el cual denotaremos $\mathbf{As}(Cay(X, \{P_i\}_{i=0}^{s})$.

Es sabido que $\mathbf{Aut}(S)$ coincide con el grupo de automorfismos del esquema de asociación $\mathbf{As}(S)$.

Teorema 1.5.19. *Sea $(X, \mathcal{R})$ un esquema de asociación de Cayley, sea G un subgrupo regular de $\mathbf{Aut}(X, \mathcal{R})$, y sea $x \in X$ un elemento arbitrario. Definimos la **proyección de Schur** de la relación básica $R_i \in \mathcal{R}$, sobre G en el punto $x \in X$ por*

$$\boldsymbol{Spr}_{G,x}(R_i) = \{h \ : \ (x^h, x) \in R_i\}.$$

Sea $P_i = \boldsymbol{Spr}_{G,x}(R_i)$, $i \in \{0, 1, \ldots, s\}$, entonces se cumple que

(i) $\{P_0, P_1, \ldots, P_s\}$ *es una partición de G con $P_0 = \{e\}$,*

(ii) si R_i es simétrico, entonces P_i también lo es,

(iii) $\boldsymbol{Spr}_{G,x^h}(R_i) = -g + \boldsymbol{Spr}_{G,x}(R_i) + g$.

Todo $y \in X$ es de la forma x^g para un único $g \in G$. Por lo tanto, de (iii) se deduce que si G es abeliano, $\boldsymbol{Spr}_{G,x}(R_i)$ no depende de la elección de x.

Teorema 1.5.20. *El espacio vectorial $\mathcal{A} = \langle\overline{P_0}, \ldots, \overline{P_s}\rangle$ es un anillo de Schur sobre G. Además, los esquemas de asociación $(X, \mathcal{R})$ y $\mathbf{As}(\mathcal{A})$ son isomorfos.*

Esto nos dice que tenemos una biyección de la forma

$$\{\text{Anillos de Schur sobre } G\} \longleftrightarrow \{\text{Esquemas de asociación de Cayley sobre } G\} \tag{1.16}$$

Mas aún, el anillo de Schur del Teorema 1.5.20 tiene las mismas constantes estructurales que el esquema $(X, \mathcal{R})$ es decir que se tiene que

$$\overline{P_i} \cdot \overline{P_j} = \sum_{k=0}^{s} c_{ij}^{k} \overline{P_k}.$$

Además se tiene que el álgebra de Bose-Mesner de $(X, \mathcal{R})$ es isomorfo al anillo $\mathcal{A}$.

Capítulo 2

Métricas

En este capítulo consideraremos la tarea de intentar clasificar las métricas sobre grupos finitos. Para ello comenzaremos con la definición básica de métrica sobre un conjunto finito X, para luego considerar el caso $X = G$, con G un grupo finito. En este caso, considerando clases de equivalencias en el espacio de métricas invariantes de G, este conjunto se convierte en un espacio finito. Si bien clasificar todas las métricas sobre un grupo dado sigue siendo una tarea complicada, ya que está relacionado con la clasificación de esquemas de asociación / anillos de Schur sobre G (lo cual no es una tarea fácil, ver [23],[69]), esta correspondencia nos permite caracterizar algunos tipos de métricas y considerar su propiedades en general.

2.1. Métricas

En esta sección se dan las nociones de métricas, pesos, grupos de simetrías, grafos asociados y nociones de equivalencias de espacios métricos. Probaremos que todo espacio semimétrico es equivalente a un espacio métrico (ver Teorema 2.1.10).

Comenzamos con la definición de distancia y peso en un conjunto finito X sin ninguna estructura adicional.

Definición 2.1.1. Sea X un conjunto y $d : X \times X \to \mathbb{R}_{\geq 0}$ una función tal que para todo $x, y, z \in X$ se cumple:

(i) $d(x,y) \geq 0$ y $d(x,y) = 0 \Leftrightarrow x = y$ (definida positiva),

(ii) $d(x,y) = d(y,x)$ (conmutativa),

(iii) $d(x,y) \leq d(x,z) + d(x,z)$ (desigualdad triangular).

Entonces diremos que d es una **distancia** y (X,d) es un **espacio métrico**. Si la función d solo cumple (i)-(ii), diremos que d es una **semimétrica** y que (X,d) es un **espacio semimétrico**. El **grupo de simetrías** de (X,d) es

$$\Gamma(X,d) = \{\sigma \in \mathbb{S}_X \,:\, d(\sigma(x),\sigma(y)) = d(x,y)\ \forall\, x,y \in X\}. \tag{2.1}$$

Las siguientes son dos de las distancias más usadas en la teoría de códigos.

Ejemplo 2.1.2. Sea $X = \{x_0, x_1, x_2, \ldots, x_{n-1}\}$ un conjunto finito. La *distancia de Hamming* en X está definida por

$$d_{Ham}(x_i,x_j) = \begin{cases} 1 & \text{si } i \neq j, \\ 0 & \text{si } i = j, \end{cases} \tag{2.2}$$

mientras que la *distancia de Lee* en X está definida por

$$d_{Lee}(x_i,x_j) = min\{|i-j|, n-|i-j|)\} \tag{2.3}$$

con $i, j = 0, \ldots, n-1$.

Observación 2.1.3. Para $\mathbb{Z}_2$ y $\mathbb{Z}_3$, las métricas de Hamming y de Lee coinciden, pero para $\mathbb{Z}_n$, con $n \geq 4$, son distintas. Por ejemplo, en $\mathbb{Z}_4$, se tiene que $d_{Ham}(0,2) = 1$ mientras que $d_{Lee}(0,2) = 2$.

En general, de ahora en adelante sólo consideraremos conjuntos finitos.

Definición 2.1.4. Sea X un conjunto y $w : X \to \mathbb{R}$ una función tal que para todo $x \in X$ cumple:

(i) $w(x) \geq 0$ (definida positiva),

(ii) $w(x) = 0$ exactamente para un único elemento de X.

Entonces diremos que w es una **función peso** y (X,w) un **espacio peso**. El **grupo de simetrías** de (X,w) es

$$\Gamma(X,w) = \{\sigma \in \mathbb{S}_X \,:\, w(\sigma(x)) = w(x)\ \forall x \in X\}.$$

Dado un espacio métrico (X,d) y $x \in X$ podemos definir canónicamente una función peso w_x de la forma

$$w_x(y) = d(y,x) \quad \forall y \in X.$$

Si $|X| = n$ entonces tenemos definidas n funciones pesos. Además, se tiene que

$$\Gamma(X,w_x) = \Gamma(X,d)_x,$$

donde $\Gamma(X,d)_x$ es el estabilizador de x en $\Gamma(X,d)$.

En particular, cuando X tiene estructura de grupo, es común definir la función peso como w_0, es decir tomar la distancia de cada elemento con respecto al cero, en cuyo caso podemos omitir el subíndice.

Ejemplo 2.1.5. Sea $X = G$ un grupo finito, el *peso de Hamming* está definido por:

$$w(x) = d_{Ham}(x,0) = \begin{cases} 1 & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases} \tag{2.4}$$

En general, si tenemos una métrica d en X, podemos extenderla naturalmente a una métrica sobre X^n. Sean $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ elementos de X^n, se define

$$d^n(x,y) = \sum_{i=1}^{n} d(x_i, y_i).$$

Tradicionalmente se hace un abuso de notación, y también se llama d a la distancia sobre X^n. Por ejemplo, la métrica de Hamming en X se extiende a X^n de esta forma para obtener la métrica mas utilizada en la teoría de códigos:

$$d^n_{Ham}(x,y) = \sum_{i=1}^{n} d_{Ham}(x_i, y_i) = |\{1 \leq i \leq n \,:\, x_i \neq y_i\}|. \tag{2.5}$$

Observación 2.1.6. Generalmente la métrica de Hamming de X extendidad a X^n también se denomina d_{Ham} en lugar de d^n_{Ham}, para evitar confusiones usaremos el superíndice n para denotar a la métrica extendida.

Grafos asociados y equivalencias de métricas

Dado un espacio métrico (X,d) podemos asociarle un grafo con pesos $\mathcal{G}(X,d) = (V,E,d)$, que llamaremos **grafo de distancias de** X, donde el conjunto de vértices es $V = X$, el conjunto de aristas es $E = X \times X$ y la función peso está dada por la distancia d, es decir el peso de la arista (x,y) es $d(x,y)$.

Observación 2.1.7. Claramente el grupo de simetrías $\Gamma(X,d)$ es exactamente el grupo $\mathbf{Aut}(\mathcal{G}(X,d))$ de automorfismos del grafo asociado.

Ejemplo 2.1.8. Los grafos de distancias de los espacio métricos $(\mathbb{Z}_4, d_{Lee})$ y $(\mathbb{Z}_2 \times \mathbb{Z}_2, d^2_{Ham})$ son

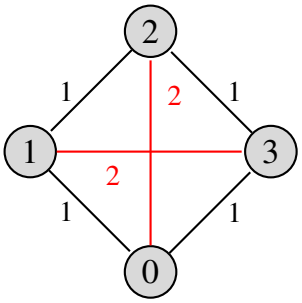


Figura 2.1: Grafo de distancias $(\mathbb{Z}_4, d_{Lee})$

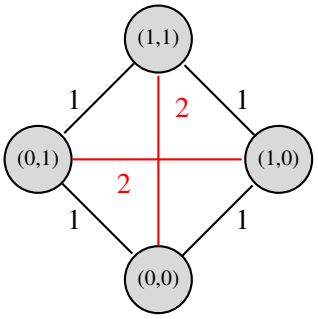


Figura 2.2: Grafo de distancias $(\mathbb{Z}_2 \times \mathbb{Z}_2, d^2_{Ham})$

Como puede verse, los dos grafos de distancias son iguales, salvo por las "etiquetas" de los vértices. Es decir, que los espacios métricos son esencialmente los mismos salvo por una identificación de los vértices.

La isometría del ejemplo anterior, conocida como el *mapa de Gray* ha sido, y es, de gran importancia en la teoría de códigos. El ejemplo nos permite ver que toda isometría se refleja en un isomorfismo de los grafos de distancias.

Equivalencias y semimétricas

Ahora definimos una noción de equivalencia entre espacios métricos.

Definición 2.1.9. Dos espacios (semi)métricos finitos (X_1, d_1) y (X_2, d_2) son **equivalentes por permutación** si existe una biyección $T : X_1 \to X_2$ tal que

$$d_1(x,y) = d_1(s,t) \Leftrightarrow d_2(T(x),T(y)) = d_2(T(s),T(t)) \quad \forall x,y,s,t \in X_1.$$

Alternativamente, si existen biyecciones $T : X_1 \to X_2$, y $\varphi : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ tales que:

$$d_1(x,y) = \varphi(d_2(T(x),T(y))) \quad \forall x,y \in X_1.$$

En particular, si $X_1 = X_2 = X$ y $T : X \to X$ es la función identidad, diremos que (X, d_1) y (X, d_2) son **equivalentes** y lo denotaremos $d_1 \sim d_2$.

Claramente, si dos espacios son equivalentes entonces

$$\Gamma(X_1, d_1) \simeq \Gamma(X_2, d_2).$$

Más aún, si $X_1 = X_2 = X$ y $d_1 \sim d_2$ se tiene que

$$\Gamma(X, d_1) = \Gamma(X, d_2).$$

Sin embargo, la recíproca no es cierta en general.

Básicamente la noción de equivalencia de semimétricas sobre un conjunto X consiste en asociar a todas las semimétricas que tienen la misma "estructura", es decir, que sus grafos asociados son isomorfos salvo un renombramiento de los pesos de las aristas.

Este concepto es necesario para trabajar con métricas sin tener que preocuparnos por la desigualdad triangular, que generalmente es la propiedad más difícil de probar. Para esto necesitaremos el siguiente resultado que nos garantiza que, de ahora en más, podremos asumir que (X,d) es un espacio métrico.

Teorema 2.1.10. *Todo espacio semimétrico finito (X,s) es equivalente a un espacio métrico (X,d).*

Demostración. Sean $p_0 = 0, p_1, \ldots, p_r$ los valores que toma la función s. Definimos los valores $q_0 = 0$ y $1 \leq q_i \leq 2$, $i = 1, \ldots, r$ y sea $d = \varphi \circ s : X \times X \to \mathbb{R}_{\geq 0}$, donde φ es la función tal que $\varphi(p_i) = q_i$, para $i = 0, \ldots, r$. Claramente, ahora se tiene que d cumple la desigualdad triangular:

$$d(x,y) \leq 2 \leq d(x,z) + d(z,y) \quad \forall x,y,z \in X, z \neq x,y.$$

Si $z = x$ ó $z = y$ la desigualdad se cumple trivialmente. Mas aún, si queremos que la función d solo tome valores enteros no negativos, podemos tomar $n \in \mathbb{N}$ tal que $r - 1 \leq n$ y entonces podemos definir los valores enteros $q_0 = 0$ y $n \leq q_i \leq 2n$ $i = 1, \ldots, r$, análogamente al caso anterior se ve que se cumple la desigualdad triangular. □

2.2. Métricas sobre grupos

Supongamos ahora que tenemos un espacio métrico (X,d) y queremos dar a X una estructura de grupo. Si $\Gamma(X,d)$ contiene un subgrupo transitivo G con $|G| = |X|$, i.e. regular, entonces podemos asociar a cada $x \in X$ un elemento $g_x \in G$, donde g_x es el único elemento de G tal que $g_x(x_0) = x$, con $x_0 \in X$ un elemento fijo. Esto nos permite definir una biyección

$$\varphi : X \to G. \tag{2.6}$$

Definición 2.2.1. Sea (X,d) un espacio métrico, y sea $G \leq \mathbb{S}_X$ tal que

$$d(\sigma(x), \sigma(y)) = d(x,y) \quad \forall x,y \in X, \sigma \in G.$$

Diremos que (X,d) es G-**invariante**, y si G actúa regularmente en X diremos que (G,d) es una G-**representación** del espacio (X,d), mediante la identificación $X \to G$ dada por la biyección φ de (2.6).

En particular, d es $\Gamma(X,d)$-invariante y existe una G-representación de (X,d) si y sólo si se tiene que $G \leq \Gamma(X,d)$ es un subgrupo regular.

Ejemplo 2.2.2. Sea (X, d_H) el espacio de Hamming con $|X| = n$, entonces $\Gamma(X, d_H) \simeq \mathbb{S}_n$, por lo tanto (X, d_H) tiene una G-representación para todo grupo finito de orden n, debido al Teorema de Cayley.

> **Nota:** De ahora en adelante (G, d) denotará un espacio métrico, con d una distancia G-invariante y G actuando por traslaciones a derecha, es decir, identificando a G con su representación regular a derecha.

Definición 2.2.3. Sea G un grupo finito, definimos el **espacio de métricas sobre G**, como el espacio de todas las métricas invariantes por traslaciones a derecha de G, al cual denotaremos $\mathcal{M}(G)$.

Notemos que $\mathcal{M}(G)$ es un conjunto infinito, por ejemplo, dada una métrica d sobre G, entonces si $a \geq 0$, se tiene que $a\,d \in \mathcal{M}(G)$, donde $a\,d$ esta definida por

$$a\,d(x,y) = a \cdot d(x,y).$$

Análogamente si $d_1, d_2 \in \mathcal{M}(G)$ entonces $d_1 + d_2 \in \mathcal{M}(G)$, con $d_1 + d_2$ definida por

$$(d_1 + d_2)(x,y) = d_1(x,y) + d_2(x,y).$$

Notar que el producto de métricas

$$(d_1 \cdot d_2)(x,y) = d_1(x,y) \cdot d_2(x,y),$$

en general no es una métrica, aunque si resulta una semimétrica.

Definición 2.2.4. Dada una métrica $d \in \mathcal{M}(G)$, podemos definir naturalmente una función peso como la distancia de $g \in G$ a e, el elemento neutro de G, es decir $w : G \to \mathbb{R}$, tal que

$$w(x) = d(x,e). \tag{2.7}$$

Definición 2.2.5. Dada un espacio métrico (G, d), podemos asociarle una partición de G, que denotaremos $\mathcal{P}(G,d)$, dada por la siguiente relación. Sean $g, h \in G$, entonces

$$g \sim h \quad \Longleftrightarrow \quad w(g) = w(h),$$

donde w es la función peso asociada a la distancia d. Llamaremos a $\mathcal{P}(G,d)$ la **partición inducida** por el espacio métrico (G, d).

Esta definición nos permitirá establecer una relación entre las métricas sobre G y las particiones inducidas, para ello estudiaremos un poco mas las propiedades de estas últimas.

Definición 2.2.6. Diremos que una partición $\mathcal{P} = P_0 | \cdots | P_s$ de un grupo finito G es **simétrica** si para todo $1 \leq i \leq s$, si $g \in P_i$ entonces $g^{-1} \in P_i$. Diremos que $\mathcal{P}$ es **unitaria** si $\{e\} \in \mathcal{P}$.

Proposición 2.2.7. *Toda partición $\mathcal{P}(G,d)$ inducida por una métrica d sobre G es simétrica y unitaria.*

Demostración. Claramente como $d(x,y) = 0$ si y sólo si $x = y$, entonces $w(x) = 0$ si y sólo si $x = e$, donde e es el elemento neutro de G, por lo tanto $\{e\} \in \mathcal{P}$, es decir que $\mathcal{P}(G,d)$ es unitaria. Ahora como la función d es simétrica, tenemos que

$$w(x) = d(x,e) = d(e,x) = w(x^{-1}),\ \forall x \in G,$$

es decir que la partición $\mathcal{P}(G,d)$ es simétrica como queríamos probar. □

En resumen, tenemos la siguiente situación:

$$\begin{array}{ccc} \{\text{Métricas sobre } G\} & \longrightarrow & \{\text{Particiones unitarias simétricas de } G\}. \\ d & \longmapsto & \mathcal{P}(G,d) \end{array} \tag{2.8}$$

Definición 2.2.8. Si d_1, d_2 son métricas sobre G, diremos que son $\mathcal{P}$-**equivalentes** si inducen la misma partición de G. Es decir, si

$$d_1 \sim_{\mathcal{P}} d_2 \iff \mathcal{P}(G,d_1) = \mathcal{P}(G,d_2). \tag{2.9}$$

A partir de ahora consideraremos el espacio

$$\mathcal{M}(G)/\sim_{\mathcal{P}}$$

de $\mathcal{P}$-clases de equivalencias de métricas sobre G.

Observación 2.2.9. Obviamente, los múltiplos escalares de una métrica d son $\mathcal{P}$-equivalente a d con $a \in \mathbb{R}_{>0}$. Sin embargo, si $d_1 \sim_{\mathcal{P}} d_1'$ y $d_2 \sim_{\mathcal{P}} d_2'$ no es cierto que $d_1 + d_2 \sim_{\mathcal{P}} d_1' + d_2'$. Por ejemplo, sea d_{Lee} la métrica de Lee sobre $\mathbb{Z}_4$ y sea d la distancia inducida por la función peso

$$w(x) = \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{si } x = 2, \\ 2 & \text{si } x = 1,3. \end{cases}$$

Claramente, se tiene que $d_{Lee} \sim_{\mathcal{P}} d$. Además, tenemos

$$\begin{aligned} d_{Lee} + d_{Lee} = 2d_{Lee} &\sim_{\mathcal{P}} d_{Lee}, \\ d_{Lee} + d = 3d_{Ham} &\sim_{\mathcal{P}} d_{Ham}. \end{aligned}$$

Sin embargo $d_{Lee} \not\sim_{\mathcal{P}} d_{Ham}$ y por lo tanto $d_{Lee} + d_{Lee} \not\sim_{\mathcal{P}} d_{Lee} + d$.

Sea $\mathcal{P}$ una partición simétrica y unitaria de G, entonces existe una métrica $d \in \mathcal{M}(G)$, tal que $\mathcal{P}(G,d) = \mathcal{P}$. Para ver esto, usaremos la misma idea que en la demostración del Teorema 2.1.10. Sea $\mathcal{P} = P_0 = \{e\}|\ldots|P_s$, definimos la siguiente función peso

$$w(x) = \begin{cases} 0 & \text{si } x = e, \\ a_i & \text{si } x \in P_i,\ i = 1,\ldots,s, \end{cases} \tag{2.10}$$

donde $a_i \in \mathbb{R}$ y $1 \leq a_i \leq 2$, para $i = 1,\ldots,s$. Ahora, podemos definir una distancia

$$d(x,y) = w(xy^{-1}).$$

Como $\mathcal{P}$ es unitaria, entonces $d(x,y) = 0$ si y sólo si $x = y$, y como es simétrica, entonces tenemos que $d(x,y) = w(xy^{-1}) = w(yx^{-1}) = d(y,x)$. Además, $d(x,y) \leq 0$, para todo $x,y \in G$, y d cumple con la desigualdad triangular pues

$$d(x,y) \leq 2 \leq d(x,z) + d(z,y) \quad \forall x,y,z \in G, z \neq x,y,$$

y en caso que $z = x$ ó $z = y$, la desigualdad se cumple trivialmente.

Observación 2.2.10. Notemos que estas consideraciones previas también nos dicen que toda función peso $w : G \to \mathbb{R}$, tal que $w(x) = w(-x)$ puede extenderse a una semimétrica, que es G-invariante, mediante la igualdad $d(x,y) = w(x-y)$.

Claramente, toda partición inducida por una métrica sobre G es simétrica y unitaria. Estas consideraciones, junto con (2.8) y la Definición 2.2.8 nos permiten dar una identificación entre $\mathcal{M}(G)/\sim_{\mathcal{P}}$ y las particiones simétricas unitarias de G. Es decir que tenemos una correspondencia

$$\{\mathcal{P}\text{-clases de métricas sobre } G\} \longleftrightarrow \{\text{Particiones simétricas unitarias de } G\}. \tag{2.11}$$

Observación 2.2.11. Es importante notar que en general, dada una partición simétrica unitaria de G, si bien podemos definir una métrica que corresponda con esa partición, no existe una forma canónica de hacerlo.

Definición 2.2.12. Si X es un conjunto y $\mathcal{P}_1$,$\mathcal{P}_2$ son particiones de X, entonces decimos que $\mathcal{P}_1$ es **más fina** que $\mathcal{P}_2$ si para todo $S \in \mathcal{P}_1$ existe un conjunto $T \in P_2$ tal que $S \subseteq T$. Denotaremos esta relación por $\mathcal{P}_1 \preceq \mathcal{P}_2$.

Notemos que el orden parcial $\preceq$ induce un retículo de particiones de G. Claramente, la correspondencia (2.11) nos permite definir un orden parcial en $\mathcal{P}$-clases de métricas de G, al que llamaremos **retículo de particiones simétricas unitarias** de G.

Observación 2.2.13. Si $G = \mathbb{Z}_n$, entonces la métrica de Lee y la métrica de Hamming son representantes de las $\mathcal{P}$-clases correspondientes al mínimo y máximo, respectivamente, del retículo $\mathcal{M}(G)/\sim_{\mathcal{P}}$.

¿Cuántas $\mathcal{P}$-clases de equivalencias de métricas existen sobre un grupo G? En vistas del Teorema 2.1.10 y de las consideraciones anteriores, la cantidad de clases de equivalencias de métricas sobre G está dada por la cantidad de particiones simétricas unitarias de G.

Definición 2.2.14. El n-ésimo número de Bell, B_n, cuenta la cantidad particiones de un conjunto de n elementos. Además satisfacen la siguiente relación recursiva

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_i.$$

Empezando con $B_0 = B_1 = 1$, los primeros números de Bell son:

1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, 190899322.

Para mas información, ver la secuencia A000110 de OEIS (The On-Line Encyclopedia of Integer Sequences) [63].

De la definición de los números de Bell y la correspondencia (2.11), tenemos el siguiente resultado.

Proposición 2.2.15. *Sea G un grupo finito y sea*

$$k = k(G) = \tfrac{1}{2}|\{g \in G : ord(g) > 2\}| + |\{g \in G : ord(g) = 2\}|.$$

Entonces, la cantidad de $\mathcal{P}$-clases de equivalencias de métricas sobre G es

$$|\mathcal{M}(G)/\sim_{\mathcal{P}}| = B_k,$$

donde B_k es el k-ésimo número de Bell.

Definición 2.2.16. Consideremos la partición $\mathcal{P}(G,d) = P_0|\ldots,|P_s$, entonces podemos asociarle un conjunto de elementos de $\mathbb{C}[G]$, de la siguiente forma

$$\bar{\mathcal{P}}(G,d) := \left\{\bar{P}_i = \sum_{g\in P_i} g \in \mathbb{C}[G]\right\}_{i=0}^{s}.$$

Sea $\mathcal{M}(G)$ el espacio de todas las métricas sobre G. Podemos pensar una métrica $d \in \mathcal{M}(G)$ como un conjunto de elementos en $\mathbb{C}[G]$ mediante la identificación

$$(G,d) \leftrightarrow \mathcal{P}(G,d) \leftrightarrow \bar{\mathcal{P}}(G,d).$$

Mediante esta identificación $(G,d_1) \sim_{\mathcal{P}} (G,d_2)$ si y sólo si $\bar{\mathcal{P}}(G,d_1)$ y $\bar{\mathcal{P}}(G,d_2)$ son iguales, y en particular generan el mismo espacio vectorial en $\mathbb{C}[G]$.

A cada métrica le asociamos una partición de G y, a su vez, ésta induce un subespacio vectorial de $\mathbb{C}[G]$. Serán de interés los casos en que la partición sea además una base de una subálgebra de $\mathbb{C}[G]$, es decir cuando sea una partición de Schur. Notemos que en este caso también tendremos que el grafo asociado $\mathcal{G}(G,d)$ será un esquema de asociación. Esto nos permitirá utilizar resultados de ambos mundos, anillos de Schur y esquemas de asociación, para aplicarlos al estudio de métricas.

Definición 2.2.17. Sea $X = \bigtimes_{i=1}^{n} X_i$, y sean d_i métricas sobre X_i, definimos la **métrica producto** en X como $d = \bigtimes_{i=1}^{n} d_i$, cuya partición correspondiente es el producto cartesiano de las particiones $\mathcal{P}_i$ correspondientes a cada d_i, es decir:

$$\mathcal{P}_{prod} \coloneqq \mathcal{P}_1 \times \cdots \times \mathcal{P}_n \coloneqq \{P_{1,m_1} \times \cdots \times P_{n,m_n} \ : \ P_{i,m_i} \in \mathcal{P}_i, i = 1,\ldots,n\}.$$

Además, si cada $X_i = Y$, y cada $d = d_i$ para $i = 1,\ldots,n$, podemos definir la **métrica producto simetrizada** en $X = Y^n$, cuya partición correspondiente es

$$\mathcal{P}_{sym} \coloneqq \left\{ \bigcup_{\sigma\in\mathbb{S}_n} P_{m_{\sigma(1)}} \times \cdots \times P_{m_{\sigma(n)}} \ : \ P_{m_i} \in \mathcal{P}, i = 1,\ldots,n \right\}.$$

Observación 2.2.18. Si tenemos la métrica de Hamming (G, d_{Ham}), entonces al considerar la métrica producto simetrizada sobre G^n, la partición obtenida coincide con la extensión natural (G^n, d^n_{Ham}). Notar que esto no vale en general para una métrica distinta de la de Hamming, es decir que no necesariamente la extensión natural coincide con la métrica producto simetrizada.

2.3. Grupos de simetrías

Todo grupo de permutación Γ actuando en G induce un anillo de Schur. El Teorema 1.5.13 nos dice que el módulo de transitividad de $\Gamma(G,d)$ es un anillo de Schur. Esto implica que dado (G,d), su grupo de simetrías $\Gamma(G,d)$ induce una partición $\mathcal{P}(G,\Gamma_e)$ de G que está dada por las órbitas de $\Gamma_e(G,d)$ (el estabilizador de $e \in G$), más aún induce un esquema de asociación schuriano. La siguiente proposición nos permitirá decir en qué casos, esa partición será simétrica.

Definición 2.3.1. Sea G un grupo abeliano e $i : G \to G$ la inversión, definida por $i(g) = g^{-1}$. Definimos el **grupo dihedral generalizado**

$$\mathbb{D}(G) = G \rtimes \langle i \rangle.$$

En el caso que $G = \mathbb{Z}_n$, el grupo cíclico de n elementos, entonces $\mathbb{D}(G) \simeq \mathbb{D}_n$, el grupo diedral para $n \geq 3$, y $\mathbb{D}(\mathbb{Z}_2) \simeq \mathbb{Z}_2$.

Es importante notar que

$$\mathbb{D}(G) \leq Hol(G) \simeq N_{\mathbb{S}_G}(G) \leq \mathbb{S}_G,$$

donde $Hol(G) = G \rtimes Aut(G)$ es el *holomorfo* de G y $N_{\mathbb{S}_G}(G)$ es el normalizador de G en $\mathbb{S}_G$, identificando a G con su representación regular a derecha. Por lo tanto, de ahora en más, pensaremos en $\mathbb{D}(G)$ como un subgrupo de $\mathbb{S}_G$, donde la inversión actúa permutando cada elemento de G por su inverso. Para más información, ver [13].

Proposición 2.3.2. *Sea (G,d) un espacio métrico, con G abeliano e $i : G \to G$ la inversión, definida por $i(g) = g^{-1}$. Entonces, i es un automorfismo que preserva distancias, por lo tanto tenemos que*

$$\mathbb{D}(G) \leq \Gamma(G,d) \leq \mathbb{S}_G.$$

Demostración. La métrica d es invariante por traslaciones, es decir que $G \leq \Gamma(G,d)$. La inversión en un grupo es un automorfismo si y sólo si G es abeliano, por lo tanto sólo resta ver que preserva las distancias. En efecto, tenemos que

$$d(a,b) = w(ab^{-1}) = w(b^{-1}a) = d(b^{-1},a^{-1}) = d(i(b),i(a)) = d(i(a),i(b)),$$

por lo tanto $\mathbb{D}(G) \leq \Gamma(G,d)$, como queríamos probar. □

Observación 2.3.3. Si $G = \mathbb{Z}_n$, entonces las métricas de Lee y Hamming, son respectivamente, representantes de la mínima y máxima clase en $\mathcal{M}(G)/\sim_{\mathcal{P}}$. Mas aún, tenemos que $\Gamma(\mathbb{Z}_n, d_{Lee}) \simeq \mathbb{D}(\mathbb{Z}_n)$ y $\Gamma(\mathbb{Z}_n, d_{Ham}) \simeq \mathbb{S}_n$.

La Proposición 2.3.2, junto con el hecho de que la órbita de e en Γ_e es trivial, nos da el siguiente resultado.

Proposición 2.3.4. *Sea G un grupo finito abeliano, entonces $\mathcal{P}(G,\Gamma_e)$ es una partición simétrica unitaria de G.*

Observación 2.3.5. Si G no es abeliano hay que tener un poco de cuidado, ya que si $\mathcal{P}$ es una partición simétrica de G, entonces no necesariamente $\mathcal{P}(G,\Gamma_e)$ va a ser simétrica. Por ejemplo, consideremos el grupo $\mathbb{D}_3 = \langle r,s \mid r^3 = 1, s^2 = 1, srs = r^{-1}\rangle$, y d, la métrica dada por la partición $\mathcal{P} = 1|r,r^{-1}|s|rs|sr$, entonces $\Gamma(\mathbb{D}_3,d) \simeq \mathbb{D}_3$, y $\mathcal{P}(\Gamma(\mathbb{D}_3,d)) = 1|r|r^{-1}|s|rs|sr$.

La Proposición 2.3.4 nos dice que en el caso que G sea abeliano, entonces dada una métrica (G,d) podemos asociarle otra métrica dada por la partición inducida por $\Gamma(G,d)$. Denotaremos a esta métrica como $\bar{d}$ y la llamaremos la **clausura schuriana** de d. Claramente tenemos que $\bar{\bar{d}} \sim_{\mathcal{P}} d$. Ahora queremos saber en qué casos se tendrá que $\bar{d} \sim_{\mathcal{P}} d$. Esto sucede si la partición inducida por d coincide con la partición dada por $\Gamma(G,d)$; y esto, a su vez, sucede si y sólo si $\mathcal{P}(G,d)$ forma un esquema de asociación schuriano.

> **Nota:** En el caso que G no sea abeliano, dada una métrica $d \in \mathcal{M}(G)$ se puede definir de la misma manera una función $\bar{d}$, pero se debe considerar que en algunos casos la partición no será simétrica, entonces $\bar{d}$ no será una *distancia*, como se puede ver en la Observación 2.3.5.

Definición 2.3.6. Ahora consideremos la siguiente relación en $\mathcal{M}(G)$:

$$d_1 \sim_\Gamma d_2 \iff \Gamma(G,d_1) = \Gamma(G,d_2). \tag{2.12}$$

En tal caso, diremos que d_1 y d_2 son Γ-equivalentes.

Definición 2.3.7. Sea $d \in \mathcal{M}(G)$. Diremos que d es una **métrica de Schur** si $\mathcal{P}(G,d)$ es una partición de Schur. En particular si $\mathcal{P}(G,d)$ es una partición de un S-anillo schuriano, diremos que d es **schuriana**.

La discusión previa asegura que dado un espacio métrico (G,d) se tiene que

$$d \sim_\Gamma \bar{d},$$

es decir, que cada Γ-clase contiene una única métrica schuriana, lo cual nos permite obtener el siguiente resultado, que nos dejará considerar métricas schurianas, en lugar de métricas en general. Además, como veremos en los siguientes capítulos, estas métricas son las que poseen ciertas propiedades más interesantes.

Proposición 2.3.8. *Sea G un grupo abeliano finito. Entonces toda métrica (G,d) es Γ-equivalente a una métrica Schuriana $(G,\bar{d})$.*

En el caso que G no sea abeliano, entonces tendremos que algunas Γ-clases podrían no contener una métrica schuriana.

Es importante notar que la relación (2.12) es mas fina que la relación (2.9). Resumiendo, tenemos la siguiente situación:

$$\begin{array}{c} (G,d) \\ \big\downarrow \mathcal{P} \\ \mathcal{P}(G,d) \\ \big\downarrow \Gamma \\ \Gamma(G,d) \end{array}$$

Es decir, que para estudiar métricas en $\mathcal{M}(G)$ vamos a considerar las Γ-clases de métricas. Esto nos lleva a tener la siguiente correspondencia:

$$\begin{array}{ccc} \{\Gamma\text{-clases de métricas}\} & \longleftrightarrow & \{\text{Particiones schurianas simétricas}\} \\ \updownarrow & & \updownarrow \\ \{\text{Grupos de simetrías}\} & \longleftrightarrow & \{\text{S-anillos simétricos schurianos}\} \end{array} \tag{2.13}$$

Es decir que considerar métricas sobre G es equivalente a considerar particiones schurianas, anillos de Schur, esquemas de asociación de Cayley o grupos de simetrías, lo cual nos ofrece una variedad de resultados para aplicar a su estudio. En la teoría de códigos, al definir una nueva métrica, una propiedad importante es que defina un esquema de asociación, pues esto garantiza, entre otras propiedades, que exista una identidad de MacWilliams que relacione el enumerador de peso de un código con el de su dual, como veremos mas adelante en este trabajo. Entonces la relación establecida nos permite tomar un esquema de asociación o anillo de Schur y definir a partir de ellos una métrica que tendrá algunas propiedades deseadas.

La relación (2.12) también nos permite obtener otra relación parcial en el conjunto de particiones simétricas de G, obteniendo asi el **retículo de simetrías** $\mathcal{L}(G)$, dándole un orden parcial al conjunto de grupos de simetrías. En el Apéndice B pueden verse los diagramas de Hasse de los reticulos de simetrías de algunos grupos cíclicos.

Métricas construidas a partir de otras

En el caso de métricas de Schur, podemos tomar todas las construcciones de anillos de Schur descriptas en la Sección 1.5 y utilizarlas para definir construcciones de métricas, que también serán métricas de Schur.

- Si $G = G_1 \times G_2$, y d_1, d_2 son métricas, en G_1 y G_2 respectivamente, inducidas por un anillo de Schur, entonces podemos definir la métricas **producto directo**

  $$d_1 \times d_2$$

  sobre G como la métrica dada por la partición correspondiente al producto directo de los anillos de Schur.

- Si $H \triangleleft G$ es un subgrupo normal, y d_1 es una métrica inducida por un anillo de Schur sobre H, y d_2 es una métrica dada por un anillo de Schur sobre G/H, entonces podemos definir la métrica **producto corona**

  $$d_1 \wr d_2$$

como la métrica dada por la partición correspondiente al producto corona de las particiones de d_1 y d_2.

- Sea $1 < K \leq H < G$ una secuencia de grupos finitos tales que $K \trianglelefteq G$. Sea d_1 una métrica sobre H y d_2 una métrica sobre G/K, cuyas particiones correspondientes cumplen las condiciones del producto cuña de anillos de Schur 1.12. Entonces podemos definir la métrica **producto cuña**

$$d_1 \wedge_K d_2$$

como la métrica dada por la partición correspondiente al producto cuña de las particiones de d_1 y d_2.

- Análogamente diremos que una métrica d sobre G es **orbital**, si su partición correspondiente induce un anillo de Schur orbital.

Calculando grupos de simetrías

Las métricas de grupos de 4 elementos

Supongamos que queremos determinar todas las posibles métricas en un grupo G con $|G| = 4$, entonces tenemos dos posibles grupos a considerar: $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

- En el caso de $\mathbb{Z}_2 \times \mathbb{Z}_2$, tenemos las siguientes particiones:

N	Partición
1	$\{(0,0)\},\{(1,0)\},\{(0,1)\},\{(1,1)\}$
2	$\{(0,0)\},\{(1,0),(0,1)\},\{(1,1)\}$
3	$\{(0,0)\},\{(0,1),(1,1)\},\{(1,0)\}$
4	$\{(0,0)\},\{(1,0),(1,1)\},\{(0,1)\}$
5	$\{(0,0)\},\{(0,1),(1,0),(1,1)\}$

cuyos grafos de distancias asociados y grupos de simetrías son, respectivamente los siguientes:

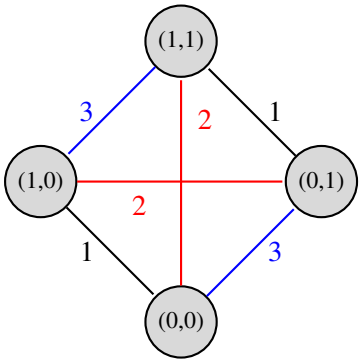


Figura 2.3: Partición 1 - Grupo de simetrías $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

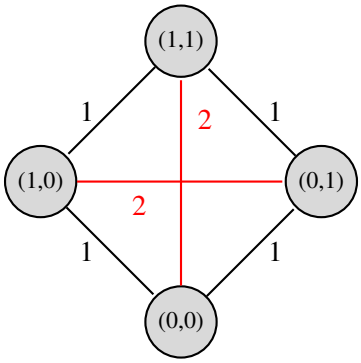


Figura 2.4: Partición 2 - Grupo de simetrías $\simeq \mathbb{D}_4$

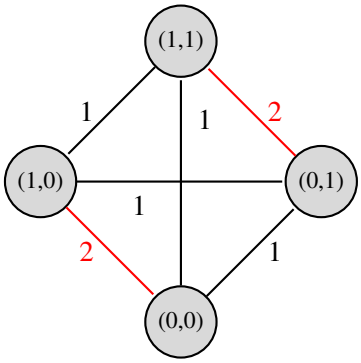


Figura 2.5: Partición 3 - Grupo de simetrías $\simeq \mathbb{D}_4$

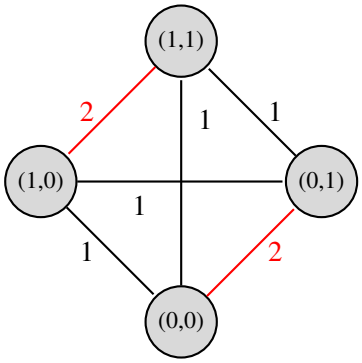


Figura 2.6: Partición 4 - Grupo de simetrías $\simeq \mathbb{D}_4$

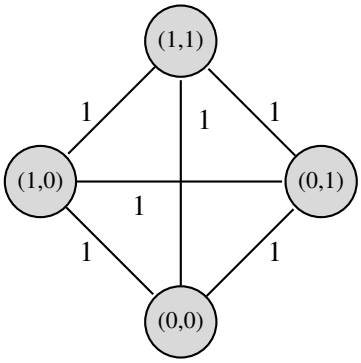


Figura 2.7: Partición 5 - Grupo de simetrías $\simeq \mathbb{S}_4$

Nota: Es importante notar que, si bien los grupos de simetrías de las métricas de las Figuras 2.4, 2.5 y 2.6 son isomorfos, estos no son iguales; es decir, que dichas métricas no están Γ-relacionadas. De ahora en más, al referirnos a un grupo de simetrías, para simplificar la notación, sólo daremos su descripción como grupo abstracto, pero es importante recordar que son grupos actuando sobre el conjunto base X.

- En el caso de $\mathbb{Z}_4$, tenemos las siguientes particiones simétricas unitarias:

N	Partición
1	$\{0\},\{1,2\},\{3\}$
2	$\{0\},\{1,2,3\}$

que se corresponden respectivamente con la métricas de Lee y de Hamming, respectivamente.

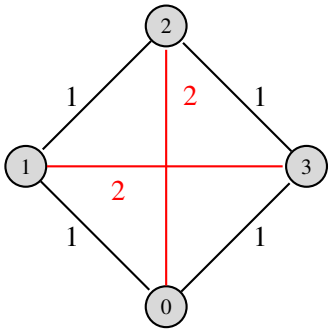


Figura 2.8: $\Gamma(\mathbb{Z}_4, d_{Lee}) \simeq \mathbb{D}_4$

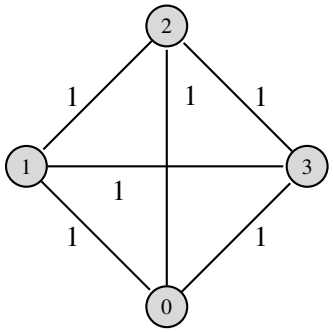


Figura 2.9: $\Gamma(\mathbb{Z}_4, d_{Ham}) \simeq \mathbb{S}_4$

Algunos grupos de simetrías

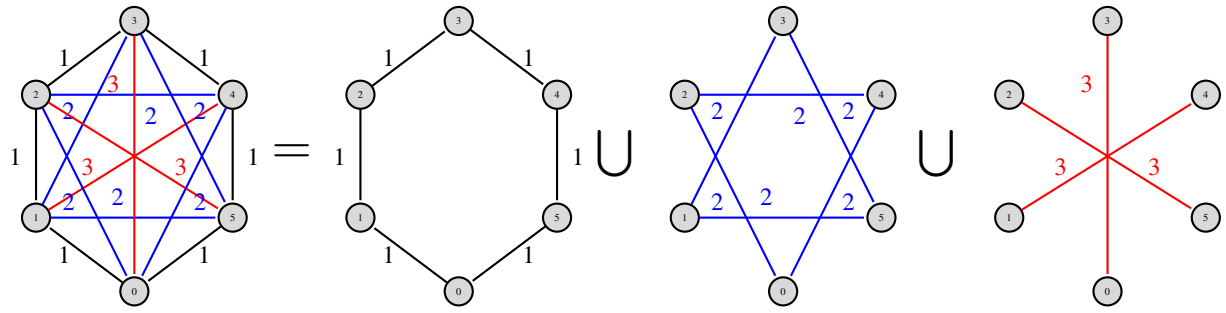
Ahora nos concentraremos en tratar de calcular los grupos de simetrías de métricas sobre grupos. Recordemos que si (G,d) es un espacio métrico,

$$\Gamma(G,d) = \mathbf{Aut}(\mathcal{G}(G,d)). \tag{2.14}$$

Teniendo en cuenta que el grafo asociado es un grafo de Cayley con etiquetas, y por lo tanto es una unión de grafos simples de Cayley, por (2.14) tenemos que

$$\Gamma(G,d) = \mathbf{Aut}(Cay(G,\mathcal{P}))) = \bigcap_{i=0}^{s} \mathbf{Aut}(G,P_i). \tag{2.15}$$

Ejemplo 2.3.9 ($\mathbb{Z}_6$)**.** Consideremos el espacio $(\mathbb{Z}_6, d_{Lee})$. La partición inducida por la métrica es $\mathcal{P} = 0 \mid 1,5 \mid 2,4 \mid 3$, entonces el siguiente es su grafo de distancias asociado, y su descomposición en grafos de Cayley simples.



$Cay(\mathbb{Z}_6, \mathcal{P})$ $Cay(\mathbb{Z}_6, \{1,5\})$ $Cay(\mathbb{Z}_6, \{2,4\})$ $Cay(\mathbb{Z}_6, \{3\})$

Utilizando la igualdad (2.15), tenemos que

$$\Gamma(\mathbb{Z}_6, d_{Lee}) = \mathbf{Aut}(Cay(\mathbb{Z}_6, \{1,5\})) \cap \mathbf{Aut}(Cay(\mathbb{Z}_6, \{2,4\})) \cap \mathbf{Aut}(Cay(\mathbb{Z}_6, \{3\})).$$

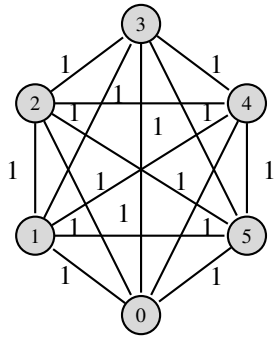
Primero notemos que $\mathbf{Aut}(Cay(\mathbb{Z}_6, \{1,5\})) \simeq \mathbb{D}_6$, las simetrías de un hexágono regular. Luego vemos que $Cay(\mathbb{Z}_6, \{2,4\})$ es isomorfo al grafo $2K_3$, es decir a dos copias disjuntas del grafo completo K_3, por lo tanto $\mathbf{Aut}(Cay(\mathbb{Z}_6, \{2,4\})) \simeq \mathbb{S}_3 \wr \mathbb{S}_2$. Análogamente $Cay(\mathbb{Z}_6, \{3\})$ es isomorfo al grafo $3K_2$, es decir a tres copias disjuntas del grafo completo K_2, por lo tanto $\mathbf{Aut}(Cay(\mathbb{Z}_6, \{3\})) \simeq \mathbb{S}_2 \wr \mathbb{S}_3$. Ahora vemos que todo automorfismo de $Cay(\mathbb{Z}_6, \{1,5\})$ también es un automorfismo de $Cay(\mathbb{Z}_6, \{2,4\})$ y de $Cay(\mathbb{Z}_6, \{3\})$, es decir que

$$\Gamma(\mathbb{Z}_6, d_{Lee}) \simeq \mathbb{D}_6.$$

Utilizando la misma idea previa podemos calcular todos los posibles grupos de simetrías de $\mathbb{Z}_6$. Para comenzar, consideremos todas las particiones correspondientes a las $\mathcal{P}$-clases de equivalencia de métricas sobre $\mathbb{Z}_6$, las cuales son:

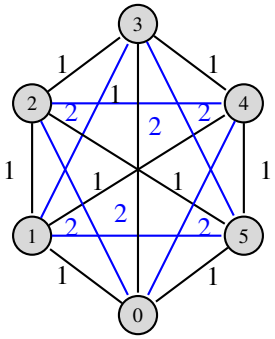
N	Partición
1	$\{0\},\{1,2,3,4,5\}$
2	$\{0\},\{1,3,5\},\{2,4\}$
3	$\{0\},\{1,2,4,5\},\{3\}$
4	$\{0\},\{1,5\},\{2,4\},\{3\}$
5	$\{0\},\{1,5\},\{2,4,3\}$

A continuación de la misma forma que antes, construimos todos los grafos asociados a cada una de las particiones, y calculamos sus grupos de simetrías.



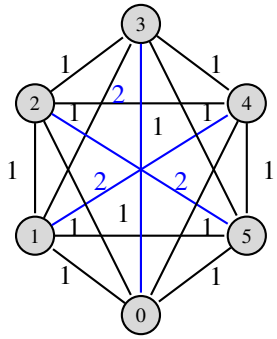
$\{0\},\{1,2,3,4,5\}$

$\mathbb{S}_6$



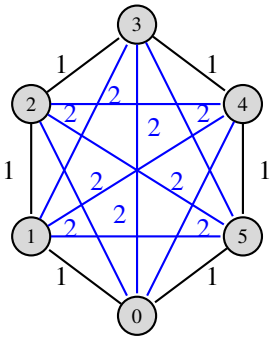
$\{0\},\{1,3,5\},\{2,4\}$

$\mathbb{S}_3 \wr \mathbb{S}_2$



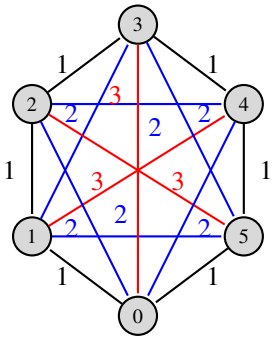
$\{0\},\{1,2,4,5\},\{3\}$

$\mathbb{S}_2 \wr \mathbb{S}_3$



$\{0\},\{1,5\},\{2,4,3\}$

$\mathbb{D}_6$



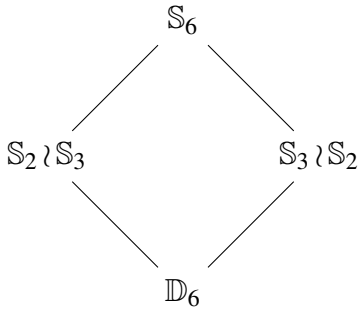
$\{0\},\{1,5\},\{2,4\},\{3\}$

$\mathbb{D}_6$

A partir de esto, podemos construir la siguiente tabla, donde podemos ver las Γ-clases de $\mathbb{Z}_6$. Además podemos notar que cada Γ-clase contiene un único elemento, excepto la clase correspondiente al grupo $\mathbb{D}_6$, la cual contiene dos particiones.

N	Partición	Grupo de simetrías
1	$\{0\},\{1,2,3,4,5\}$	$\mathbb{S}_6$
2	$\{0\},\{1,3,5\},\{2,4\}$	$\mathbb{S}_3 \wr \mathbb{S}_2$
3	$\{0\},\{1,2,4,5\},\{3\}$	$\mathbb{S}_2 \wr \mathbb{S}_3$
4	$\{0\},\{1,5\},\{2,4,3\}$	$\mathbb{D}_6$
5	$\{0\},\{1,5\},\{2,4\},\{3\}$	

Así también podemos construir el retículo de simetrías de $\mathbb{Z}_6$.



Ejemplo 2.3.10 ($\mathbb{S}_3$)**.** Ahora consideremos el grupo de simetrías

$$\mathbb{S}_3 = \{(1),(2,3),(1,2),(1,2,3),(1,3,2),(1,3)\}.$$

El cardinal de $\mathcal{M}(\mathbb{S}_3)$, según la Teorema 2.2.15 es

$$|\mathcal{M}(\mathbb{S}_3)| = B_4 = 15.$$

Utilizando la misma metodología que en el ejemplo anterior, haciendo cálculos en computadora podemos obtener las Γ-clases de métricas sobre $\mathbb{S}_3$ que podemos ver en la siguiente tabla.

Métricas schurianas sobre $\mathbb{S}_3$

N	Partición	Grupo de Simetrías
1	$\{(1)\},\{(2,3),(1,2),(1,2,3),(1,3,2),(1,3)\}$	$\mathbb{S}_6$
2	$\{(1)\},\{(2,3),(1,3),(1,2)\},\{(1,2,3),(1,3,2)\}$	$\mathbb{S}_3 \wr \mathbb{S}_2$
3	$\{(1)\},\{(1,3),(2,3),(1,3,2),(1,2,3)\},\{(1,2)\}$	$\mathbb{S}_2 \wr \mathbb{S}_3$
$3'$	$\{(1)\},\{(1,2),(2,3),(1,3,2),(1,2,3)\},\{(1,3)\}$	$\mathbb{S}_2 \wr \mathbb{S}_3{}'$
$3''$	$\{(1)\},\{(1,2),(1,3),(1,3,2),(1,2,3)\},\{(2,3)\}$	$\mathbb{S}_2 \wr \mathbb{S}_3{}''$
4	$\{(1)\},\{(2,3),(1,3)\},\{(1,2,3),(1,3,2)\},\{(1,2)\}$	$\mathbb{D}_6$
$4'$	$\{(1)\},\{(1,2),(2,3)\},\{(1,2,3),(1,3,2)\},\{(1,3)\}$	$\mathbb{D}_6{}'$
$4''$	$\{(1)\},\{(1,2),(1,3)\},\{(1,2,3),(1,3,2)\},\{(2,3)\}$	$\mathbb{D}_6{}''$

En este caso podemos ver que a diferencia del caso de $\mathbb{Z}_6$ (y de $\mathbb{Z}_n$ en general), existen distintas Γ≈clases de métricas cuyos grupos de simetrías son isomorfos. Además, como se vio anteriormente en la Observación 2.3.5, en este caso la Γ-clase de la partición

$$\{(1)\},\{(1,2)\},\{(1,3)\},\{(1,2,3),(1,3,2)\},\{(2,3)\},$$

no contiene una métrica schuriana, porque la partición $\mathcal{P}(G,\Gamma_e)$, en este caso resulta ser

$$\{(1)\},\{(1,2)\},\{(1,3)\},\{(1,2,3)\}\{(1,3,2)\},\{(2,3)\},$$

la cual no es simétrica, y por lo tanto no es posible definir una métrica correspondiente.

Ejemplo 2.3.11 ($\mathcal{Q}_8$)**.** Sea $\mathcal{Q}_8$, el grupo de cuaterniones, es decir,

$$\mathcal{Q}_8 = \{1,-1,i,-i,j,-j,k,-k\}$$

con el producto definido por las relaciones

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k,$$
$$kj = -i, \quad ik = -j, \quad i^2 = j^2 = k^2 = -1.$$

Entonces la siguiente tabla muestra todas las métricas $\mathcal{Q}_8$-invariantes, con sus particiones de Schur correspondientes a cada clase y sus grupos de simetrías correspondientes.

Métricas schurianas sobre $\mathcal{Q}_8$ (salvo isomorfismos)

N	Particiones de Schur	Grupo de Simetrías
1	$\{1\},\{-1,i,-i,j,-j,k,-k\}$	$\mathbb{S}_8$
2	$\{1\},\{i,-1,-i\},\{j,-j,k,-k\}$	$\mathbb{S}_4 \wr \mathbb{S}_2$
3	$\{1\},\{-1\},\{i,-i,j,-j,k,-k\}$	$\mathbb{S}_2 \wr \mathbb{S}_4$
4	$\{1\},\{i,-i\},\{-1\},\{j,-jk,-k\}$	$\mathbb{D}_4 \wr \mathbb{S}_2$
5	$\{1\},\{i,-i\},\{-1\},\{j,-j\},\{k,-k\}$	$\mathbb{S}_2 \wr (\mathbb{S}_2 \times \mathbb{S}_2)$

Algunos resultados sobre el grupo de isometrías

En esta sección mostraremos algunos resultados conocidos sobre grupos de simetrías, así como también usaremos algunos resultados de anillos de Schur para determinar la estructura de las métricas schurianas sobre $\mathbb{Z}_n$. El siguiente resultado es consecuencia de [42, Thm. 2.4].

Proposición 2.3.12. *Sea (G,d) una métrica de Schur, de tipo producto directo en $G = \bigtimes G_i$, entonces*

$$\Gamma(G,d) \simeq \prod_{i=1}^{n} \Gamma(G_i,d_i).$$

Proposición 2.3.13. *Sea (G,d) una métrica producto simetrizada en $G = \prod_{i=1}^{m} H$, entonces*

$$\Gamma(G,d) \simeq \Gamma(H,d_H) \wr \mathbb{S}_m.$$

Gracias a la Proposición anterior y a la Observación 2.2.18 podemos obtener el siguiente resultado, ya conocido en la literatura.

Proposición 2.3.14. *Sea (X, d_{Ham}^n) el espacio de Hamming, con $|X| = m$, entonces*

$$\Gamma(X, d_{Ham}^n) \simeq \mathbb{S}_m \wr \mathbb{S}_n.$$

2.3.1. Métricas sobre $\mathbb{Z}_n$

Finalizamos esta sección caracterizando todas las métricas schurianas sobre $\mathbb{Z}_p$ y daremos una descripción sobre el caso de métricas schurianas sobre $\mathbb{Z}_n$.

Gracias al Corolario 1.5.10, que nos dice que todo anillo de Schur sobre $\mathbb{Z}_n$ es orbital, podemos deducir el siguiente resultado.

Teorema 2.3.15. *Sea $G = \mathbb{Z}_p$ con p primo, entonces toda métrica schuriana sobre $\mathbb{Z}_p$ es de la forma*

$$\mathbb{C}[\mathbb{Z}_p]^{\mathcal{H}} \quad con \quad \langle i \rangle \leq \mathcal{H} \leq Aut(\mathbb{Z}_p).$$

En este caso, sobre $\mathbb{Z}_p$ se tiene que todos los anillos de Schur son schurianos, es decir que toda métrica de Schur es schuriana. En particular, se corresponden con los siguientes grupos de simetrías.

Teorema 2.3.16. *Sea $G = \mathbb{Z}_p$ con p primo, todos los grupos de simetrías de G son de la forma:*

(i) $\Gamma(G,d) \simeq \mathbb{S}_p$.

(ii) $\Gamma(G,d) \simeq \mathbb{Z}_p \rtimes \mathcal{H}$, *con* $\langle i \rangle \leq \mathcal{H} < Aut(\mathbb{Z}_p)$, $|\mathcal{H}|$ *par. En particular tomando* $\mathcal{H} = \langle i \rangle$ *se obtiene el grupo de simetrías* $\mathbb{D}_p$.

Corolario 2.3.17. *Sea $G = \mathbb{Z}_p$ con p primo, entonces existen tantas métricas schurianas sobre $\mathbb{Z}_p$ como divisores pares de $p-1$.*

Demostración. Según el Teorema 2.3.15, cada métrica schuriana se corresponde con un subgrupo $\mathcal{H}$, tal que $\langle i \rangle \leq \mathcal{H} \leq Aut(\mathbb{Z}_p)$. Sabiendo que $Aut(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$ y que entonces $2 \leq |\mathcal{H}| \leq p-1$, se obtiene el resultado buscado. □

Ejemplo 2.3.18 ($\mathbb{Z}_{13}$)**.** Utilizando el Teorema 2.3.16, y sabiendo que $Aut(\mathbb{Z}_{13}) \simeq \mathbb{Z}_{12}$, podemos determinar las Γ-clases de métricas sobre $\mathbb{Z}_{13}$

Métricas sobre $\mathbb{Z}_{13}$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12\}$	$\mathbb{S}_{13}$
2	$\{0\},\{1,3,4,9,10,12\},\{2,5,6,7,8,11\}$	$\mathbb{Z}_{13} \rtimes \mathbb{Z}_6$
3	$\{0\},\{1,5,8,12\},\{2,3,10,11\},\{4,6,7,9\}$	$\mathbb{Z}_{13} \rtimes \mathbb{Z}_4$
4	$\{0\},\{1,12\},\{2,11\},\{3,10\},\{4,9\},\{5,8\},\{6,7\}$	$\mathbb{D}_{13}$

Más en general, el Corolario 1.5.8, nos dice que todo anillo de Schur sobre $\mathbb{Z}_n$ es trivial, orbital, producto directo, producto corona o producto cuña de anillos de Schur.

Teorema 2.3.19. *Toda métrica de Schur sobre $\mathbb{Z}_n$ es de tipo trivial orbital, producto directo, producto corona o producto cuña.*

Debemos notar que en general $\mathbb{Z}_n$ no es un grupo de Schur (ver 1.5.15), es decir que no todas las métricas de Schur van a ser schurianas, pero es sabido que $\mathbb{Z}_n$ es un grupo de Schur para $n < 72$.

Este Teorema, junto con las consideraciones previas sobre grupos de simetrías nos permiten calcular las métricas schurianas sobre $\mathbb{Z}_n$. En el Apéndice A damos todas las métricas schurianas de $\mathbb{Z}_n$, con $n \leq 20$.

Métrica a partir de particiones

Ahora consideremos que dado un grupo G y una partición de Schur de tipo producto corona, y queremos determinar Si $H \triangleleft G$ es un subgrupo normal, y d_1 es una métrica inducida por un anillo de Schur sobre H, y d_2 es una métrica dada por un anillo de Schur sobre G/H, entonces queremos construir una métrica correspondiente a la clase de la partición de

$$d_1 \wr d_2.$$

Vamos a definir la distancia $d(x,y) = w(x-y)$ por

$$w(x) = \begin{cases} w_1(x) & \text{si } x \in H, \\ r + w_2(\bar{x}) & \text{si } x \notin H, \end{cases} \tag{2.16}$$

donde $r = \max_{h \in H}\{w(h)\}$ y $\bar{x}$ es la imagen de x en G/H mediante la proyección canónica. Es fácil ver que d es simétrica, que $d(x,y) \leq 0$ y $d(x,y) = 0 \iff x = y$, sólo resta probar que d cumple la desigualdad triangular.

$$w(x+y) = \begin{cases} w_1(x+1) & \text{si } x+y \in H, \\ r + w_2(\overline{x+y}) & \text{si } x+y \notin H, \end{cases} \tag{2.17}$$

En el primer caso, si $x, y \in H$, entonces

$$w(x+y) = w_1(x+y) \leq w_1(x) + w_2(y) = w(x) + w(y),$$

si $x \in H$, e $y \notin H$

$$w(x+y) = r + w_2(\overline{x+y}) = r + w_2(\bar{y}) = w(y) \leq w(x) + w(y),$$

si $x, y \notin H$, y $x+y \in H$

$$w(x+y) = w_1(x+y) \leq r \leq r + w_2(\bar{x}) + r + w_2(\bar{y}) = w(x) + w(y),$$

si $x,y \notin H$, y $x+ynot \in H$

$$w(x+y) = r + w_2(\overline{x+y}) \leq r + w_2(\bar{x}) + w_2(\bar{y}) \leq r + w_2(\bar{x}) + r + w_2(\bar{y}) = w(x) + w(y).$$

Ejemplo 2.3.20. En el Ejemplo 2.3.9 determinamos todos los tipos de métricas schurianas sobre el grupo $\mathbb{Z}_6$. Ahora vamos a construir explícitamente métricas correspondientes a cada una de esas clases. Consideremos la partición dada por

$$\{0\},\{1,3,5\},\{2,4\}$$

Definimos $d_1(x,y) = w_1(x-y)$, con

$$w_1(x) = \begin{cases} w_{Ham,2}(x) & \text{si } x \in 2\mathbb{Z}_6, \\ 1 + w_{Ham,3}(\bar{x}) & \text{si } x \notin 2\mathbb{Z}_6. \end{cases} \tag{2.18}$$

Es decir que $w_1(0) = 0$, $w_1(2) = w_1(4) = 1$ y $w_1(1) = w_1(3) = w_1(5) = 2$.

Ahora tomando la partición

$$\{0\},\{1,2,4,5\},\{3\}$$

podemos definir análogamente la distancia $d_2(x,y) = w_1(x-y)$, con

$$w_2(x) = \begin{cases} w_{Ham,3}(x) & \text{si } x \in 3\mathbb{Z}_6, \\ 1 + w_{Ham,2}(\bar{x}) & \text{si } x \notin 3\mathbb{Z}_6. \end{cases} \tag{2.19}$$

Es decir que $w_2(0) = 0$, $w_2(3) = 1$ y $w_2(1) = w_2(2) = w_2(4) = w_2(5) = 2$.

Finalmente, podemos ver que d_{Lee}, d_1, d_2 y d_{Ham} son representantes explícitos de las clases de simetrías de $\mathbb{Z}_6$.

N	Partición	Grupo de simetrías	Métrica
1	{0},{1,2,3,4,5}	$\mathbb{S}_6$	d_{Ham}
2	{0},{1,3,5},{2,4}	$\mathbb{S}_3 \wr \mathbb{S}_2$	d_1
3	{0},{1,2,4,5},{3}	$\mathbb{S}_2 \wr \mathbb{S}_3$	d_2
4	{0},{1,5},{2,4,3}	$\mathbb{D}_6$	d_{Lee}

2.4. Métricas sobre anillos

Toda métrica sobre un anillo R, también es una métrica sobre el grupo base R^+, pero si además exigimos la condición de que la métrica sea invariante por multiplicación de los elementos de $\mathcal{U}(R)$, el grupo de unidades de R, tenemos que el espacio de todas las métricas sobre R, $\mathcal{M}(R)$ es un subconjunto de las métricas sobre R^+, el grupo base del anillo R, i.e.

$$\mathcal{M}(R) \subset \mathcal{M}(R^+).$$

Tradicionalmente el estudio de códigos comenzó con códigos lineales sobre $\mathbb{F}_q$, es decir subespacios de $\mathbb{F}_q^n$ para algún n, y luego se extendió al estudio de códigos sobre un anillo con unidad finito R; donde un código *lineal* sobre R es un R-submódulo de R^n, para algún n.

A continuación veremos algunos ejemplos de las métricas más estudiadas en la Teoría de Códigos sobre anillos.

Un anillo finito R se dice de **Frobenius** si

$$R/Rad(R) \cong Soc(R),$$

como módulo a izquierda o a derecha, donde $Rad(R)$ es el *radical* de R, la intersección de todos los ideales maximales a izquierda (a derecha) y $Soc(R)$ es el *sócalo* de R, la suma de todos los submódulos simples a izquierda (a derecha). Equivalentemente, R es Frobenius si su módulo de caracteres $\widehat{R}$ es isomorfo a R como módulo a izquierda o a derecha (ver Definición 4.2.5). Para más información sobre por qué esta clase de anillos son importantes para la teoría de códigos, recomendamos leer [65].

Peso homogéneo

Definición 2.4.1. Sea R un anillo. Una función $w : R \to \mathbb{R}_{\geq 0}$ se dice **peso homogéneo a izquierda** si $w(0) = 0$ y además

(i) si $Rx = Ry$, entonces $w(x) = w(y)$, para $x, y \in R$;

(ii) para todo $x \in R$, $x \neq 0$ se tiene $\sum_{y \in Rx} w(y) = \gamma |Rx|$, para un cierto $\gamma \in \mathbb{R}_{>0}$.

Diremos que w tiene **promedio** γ, y diremos que el peso es **normalizado** si $\gamma = 1$.

Si R es Frobenius, los pesos homogéneos están caracterizados.

Lema 2.4.2. *Sea R un anillo de Frobenius finito, y sea χ un carácter generador de $\hat{R}$. Entonces una*

función peso $w : R \to \mathbb{R}$ es homogénea con promedio $\gamma > 0$ si y sólo si

$$w(x) = \gamma\Big\{1 - \frac{1}{|Rx|}\sum_{u\in R^*}\chi(ux)\Big\}. \tag{2.20}$$

Ejemplo 2.4.3. Sea $R = GR(p^r, m)$ un anillo de Galois finito. R es un anillo de Frobenius. Entonces el peso homogéneo en (2.20) toma la forma

$$w(x) = \begin{cases} \gamma & \text{si } x \notin Soc(R), \\ \gamma\frac{q}{q-1} & \text{si } x \in Soc(R),\ x \neq 0, \\ 0 & \text{si } x = 0. \end{cases} \tag{2.21}$$

En el caso particular en que $R = GF(q) = \mathbb{F}_q$, tenemos $w(x) = \gamma\frac{q}{q-1}w_H(x)$, es decir, un múltiplo del peso de Hamming.

Peso egalitario

Definición 2.4.4. Sea R un anillo de Frobenius con carácter generador χ. Para cada subgrupo $U \subseteq \mathcal{U}(R)$ y cada $\gamma \in \mathbb{R}$, definimos una función peso $w_U : R \to \mathbb{R}_{\geq 0}$ de la forma

$$w_U(a) = \gamma\Big\{1 - \frac{1}{|U|}\sum_{u\in U}\chi(au)\Big\}.$$

Tal función w_U se dice que es un *peso egalitario*. Más aún, si $I \subset R$ es un submódulo no nulo, y $r_0 \in R$, entonces

$$\sum_{a\in I} w_U(r_0 + a) = \gamma|I|.$$

Es decir, que la propiedad egalitaria se aplica a todos los cosets de los submódulos de R. Si $U = \mathcal{U}$, entonces $w_{\mathcal{U}}$ es la métrica homogénea.

Capítulo 3

Métricas Poset

Las métricas poset surgieron como una forma de generalizar el espacio métrico de Hamming $(\mathbb{F}_q^n, d_{Ham})$. Fueron introducidas por Brualdi et al. en [7], y desde ese momento comenzaron a ser estudiadas en profundidad tratando de obtener resultados similares al caso de Hamming. En este capítulo, daremos su definición, junto con algunas propiedades básicas, para luego centrarnos en métricas poset inducidas por una familia especial de posets, los posets jerárquicos. En este caso, calcularemos el grupo de simetrías del espacio $(\mathbb{F}_q^n, d_P)$, generalizando asi resultados previos.

3.1. Posets y métricas asociadas

Aunque el concepto de conjuntos parcialmente ordenados es mucho más amplio, sólo consideraremos órdenes parciales sobre conjuntos finitos. Sin pérdida de generalidad, consideraremos posets sobre el conjunto $[n] = \{1, 2, \ldots, n\}$.

Algunas definiciones básicas

Definición 3.1.1. Diremos que $P = ([n], \preceq_P)$ es un **conjunto parcialmente ordenado** (también conocido como *poset*), si $\preceq_P$ es una relación de orden parcial en $[n]$, es decir, si para todo $a, b, c \in [n]$ se tiene que:

- $a \preceq_P a$,
- si $a \preceq_P b$ y $b \preceq_P c$, entonces $a \preceq_P c$,
- si $a \preceq_P b$ y $b \preceq_P a$, entonces $a = b$.

Un **ideal** en un poset $P = ([n], \preceq_P)$ es un subconjunto $I \subseteq [n]$ tal que, dados $a \in [n]$ y $b \in I$, si $a \preceq_P b$, entonces $a \in I$. Dado $A \subseteq [n]$, denotamos como $\langle A \rangle_P$ al mínimo ideal P que contiene a A y lo llamamos el **ideal generado por** A. Un ideal $\langle \{a\} \rangle_P$ generado por un conjunto $A = \{a\}$ con un solo

elemento se denomina **ideal primo**. Denotamos, para simplificar, $\langle a \rangle_P = \langle \{a\} \rangle_P$. Un elemento a de un ideal $I \subseteq [n]$ se dice **maximal** en I si $a \preceq_P x$ para algún $x \in I$ implica que $x = a$. El conjunto de todos los elementos maximales de un ideal I se denota $\mathcal{M}_P(I)$.

Es fácil ver que dado un ideal $I \subseteq [n]$, $\mathcal{M}_P(I)$ es el mínimo conjunto tal que $\langle \mathcal{M}_P(I) \rangle_P = I$. Además, un ideal es primo si y sólo si contiene un único elemento maximal. Mas aún, este elemento maximal es también el generador.

Diremos que b **cubre** a a si $a \preceq_P b$, $a \neq b$ y no existe ningún $c \in [n]$ tal que $a \preceq_P c \preceq_P b$. Una buena forma de considerar las propiedades de un poset, es mediante una representación, llamada **diagrama de Hasse** del poset $P = ([n], \preceq_P)$. El diagrama de Hasse es un grafo dirigido cuyos vértices son los elementos de $[n]$ y una arista conecta b con a si y sólo si b cubre a. Al graficarlo, asumimos que b esta "arriba de" a si b cubre a a por lo tanto la dirección siempre es asumida hacia abajo.

La métrica poset

En el contexto de la Teoría de Códigos, un poset $P = ([n], \preceq_P)$ nos permite definir una métrica que en algún sentido generaliza a la métrica de Hamming. Sea $\mathbb{F}_q^n$ el espacio vectorial de dimensión n sobre el cuerpo finito $\mathbb{F}_q$. Dado $u \in \mathbb{F}_q^n$, el **soporte** y el P**-peso** de u están definidos por

$$\operatorname{supp}(u) = \{i \in [n] : u_i \neq 0\} \qquad \text{y} \qquad w_P(u) = |\langle \operatorname{supp}(u) \rangle_P|,$$

donde $|\cdot|$ denota la cardinalidad del conjunto dado. Para simplificar, el conjunto de elementos maximales en el ideal generado por $\operatorname{supp}(u)$ lo denotaremos por $\mathcal{M}_P(u)$.

Definición 3.1.2. La **métrica poset** en $\mathbb{F}_q^n$ se define por

$$d_P(u,v) = w_P(u-v)$$

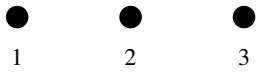
para $u, v \in \mathbb{F}_q^n$. El espacio métrico $(\mathbb{F}_q^n, d_P)$, se denomina P**-spacio**.

Observación 3.1.3. Si bien la métrica poset se define sobre el espacio $\mathbb{F}_q^n$, considerando que para su definición solo se usa la estructura aditiva del espacio vectorial, la misma definición nos permite definir una métrica poset sobre G^n para cualquier grupo finito G e incluso para un producto de grupos $G = G_1 \times \cdots \times G_n$ ([21]) o sobre R^n, donde R es un anillo de Frobenius ([3]).

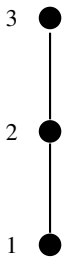
Cadenas y anticadenas

Una **anti-cadena** es un poset P con un conjunto mínimo de relaciones, i.e., para todo $a \neq b \in [n]$, entonces no es cierto que $a \preceq_P b$ ni $b \preceq_P a$. Considerando una anticadena, tenemos $\langle \operatorname{supp}(u) \rangle_P = \operatorname{supp}(u)$, por lo tanto induce la ya conocida métrica de Hamming. Además del poset anticadena, existe otro poset que puede ser considerado extremo, aquel que tiene el máximo número de relaciones, el

poset cadena. En este caso, dos elementos de $[n]$ son **comparables** (o están **relacionados**), i.e., dados $a, b \in [n]$, entonces se tiene que $a \preceq_P b$ o $b \preceq_P a$.



Anticadena en $[3]$



Cadena en $[3]$, $1 \preceq 2 \preceq 3$

Estos dos posets, la cadena y la anticadena, siendo determinados por una máxima o mínima cantidad de relaciones, también dan origen a métricas que son, en algún sentido, extremas. La métrica de Hamming, determinada por una anticadena, es el análogo discreto del espacio Euclídeo, el cual modela nuestra percepción del mundo. El poset cadena, por otro lado, determina un tipo diferente de métricas, conocidas como *ultra-métricas*, donde la desigualdad triangular

$$d(x,z) \leq d(x,y) + d(y,z)$$

es reemplazada por una desigualdad más restrictiva

$$d(x,z) \leq \text{máx}\{d(x,y), d(y,z)\}.$$

Esta condición tiene un gran impacto en la métrica; considerando la métrica dada por una cadena, la fórmula para el radio de empaquetamiento de un código es $d(\mathcal{C}) - 1$ y no el usual $\lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$, donde $d(\mathcal{C})$ es la distancia mínima (ver [33] para más detalles).

A pesar del hecho de que la métrica inducida por una cadena parece desafiar nuestra intuición, es en realidad relativamente simple y la geometría de los códigos bajo esta métrica fue descripta en detalle en [33], incluyendo la caracterización de los códigos perfectos y los códigos MDS.

En el caso general, el comportamiento determinando por cadenas y anticadenas se mezcla, y calcular los invariantes geométricos de un código se convierte en una tarea difícil, por lo tanto se comenzó a considerar diferentes formas de combinar esos dos posets. Realizando uniones disjuntas de cadenas finitas o relacionando (jerárquicamente) familias de anticadenas, obtenemos dos de las familias de métricas posets más estudiadas: la métrica de Niederreiter-Rosembloom-Tsfasman (NRT) y la familia de posets jerárquicos.

Métricas NRT

Consideremos la siguiente métrica en $\mathbb{F}_q^n$. Sean $x, y \in \mathbb{F}_q^n$, entonces

$$d_{RT}(x,y) = \max_{1 \leq i \leq n} \{i \,:\, x_i - y_i \neq 0\}.$$

No es difícil ver que esta métrica coincide con la métrica poset en $\mathbb{F}_q^n$ dada por el poset cadena $1 \preceq 2 \preceq \cdots \preceq n$.

$$d_P(x,y) = |\langle supp(x-y)\rangle_P| = \max_{1 \leq i \leq n} \{i \,:\, x_i - y_i \neq 0\}. \tag{3.1}$$

Las métricas NRT, también llamadas métricas de Rosenbloom- Tsfasman generalizadas, están determinadas por un poset que es la unión disjunta de cadenas. Han sido investigados en varios trabajos, por ejemplo [52], [53], [47] y [62].

Métricas de posets jerárquicos

Los posets jerárquicos, que son un gran tema de estudio, corresponden a otra posible generalización de las cadenas y anticadenas. Antes de definir un poset jerárquico, podemos decir que las métricas inducidas por ellos son una verdadera generalización de la métrica de Hamming en varios aspectos. Sólo como ejemplo, las únicas métricas poset donde la distancia mínima de un código determina el radio de empaquetamiento son aquellas inducidas por un poset jerárquico. Ahora daremos algunos conceptos necesarios para definir los posets jerárquicos.

La **altura** $h(a)$ de un elemento $a \in P$ es el cardinal de la cadena más larga que tiene a a como elemento maximal. La **altura** $h(P)$ de un poset es el maximo de las alturas de sus elementos, i.e.,

$$h(P) = \max\{h(a) : a \in [n]\}.$$

El **nivel i-ésimo** Γ_i^P de un poset P es el conjunto de todos los elementos de altura i, i.e.,

$$\Gamma_i^P = \{a \in [n] : h(a) = i\}.$$

Observemos que cada nivel de un poset tiene la estructura de orden de una anticadena.

Definición 3.1.4. Un poset $P = ([n], \preceq_P)$ se dice **jerárquico** si los elementos de distintos niveles (anticadenas) son siempre comparables, es decir, si $a \in \Gamma_i^P$ y $b \in \Gamma_j^P$, entonces $a \preceq_P b$ si y sólo si $i < j$. Un **espacio jerárquico** es un P-espacio, con P un poset jerárquico.

Ahora definimos poset jerárquico con niveles.

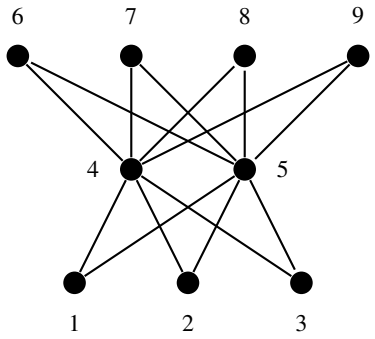
Definición 3.1.5. Sean $n_1, n_2, \ldots, n_t$ números naturales con $n_1 + n_2 + \cdots + n_t = n$. El **poset jerárquico con t niveles y n elementos**, que denotamos por $\mathbb{H}(n; n_1, \ldots, n_t)$, es el poset definido en el conjunto

$\{(i,j) \,:\, 1 \leq i \leq t, 1 \leq j \leq n_i\}$ por la relación de orden

$$(i,j) < (l,m) \quad \Leftrightarrow \quad i < l.$$

En particular el poset $\mathbb{H}(n;1,\ldots,1)$ es una cadena de altura n y el poset $\mathbb{H}(n;n)$ es una anticadena de n elementos, que también puede denotarse como $\mathbf{n}$.

Ejemplo 3.1.6. El siguiente gráfico muestra el diagrama de Hasse del poset jerárquico $\mathbb{H}(9;3,2,4)$



De ahora en adelante, si no se presenta ninguna confusión, omitiremos P como superíndice en Γ_i^P y como subíndice en $\preceq_P$, $\langle\cdot\rangle_P$, y w_P.

Opereaciones de posets

A continuación definiremos algunas operaciones sobre posets que serán de utilidad en las próximas secciones.

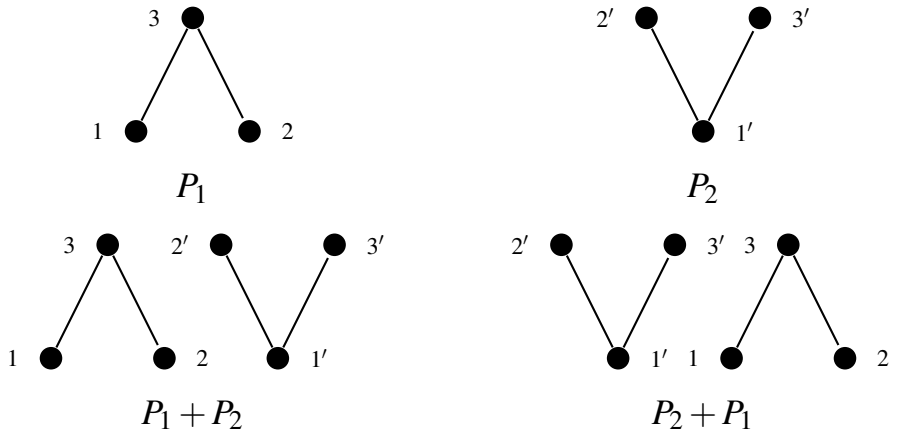
Definición 3.1.7. Sean $P_1 = ([n_1], \preceq_{P_1})$ y $P_2 = ([n_2], \preceq_{P_2})$ dos posets. Definimos la **suma** o **unión disjunta** $P_1 + P_2$, como el orden parcial sobre $[n_1] \cup [n_2]$ (unión disjunta) dado por las relaciones:

(i) si $i, j \in [n_1]$ y $i \preceq j$ en P_1, entonces $i \preceq j$ en $P_1 + P_2$,

(ii) si $i, j \in [n_2]$ y $i \preceq j$ en P_2, entonces $i \preceq j$ en $P_1 + P_2$.

Podemos notar que esta operación de posets es asociativa y conmutativa. Visualmente, el diagrama de Hasse de la unión disjunta de posets se puede obtener yuxtaponiendo los dos diagramas de Hasse de cada uno de los posets, como podemos er en el siguiente ejemplo.

Ejemplo 3.1.8. En la siguiente figura podemos ver la unión disjunta de los posets P_1 y P_2, dados por sus respectivos diagramas de Hasse.



Definición 3.1.9. Sean $P_1 = ([n_1], \preceq_{P_1})$ y $P_2 = ([n_2], \preceq_{P_2})$, dos posets, definimos la **suma ordinal** $P_1 \oplus P_2$, como el orden parcial sobre $[n_1] \cup [n_2]$(unión disjunta) dado por las relaciones:

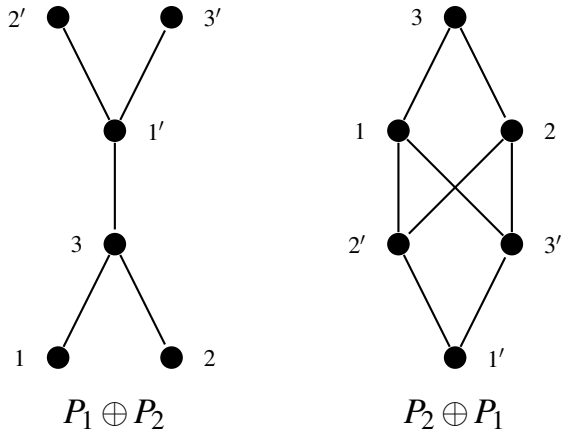
(i) si $i, j \in [n_1]$ y $i \preceq j$ en P_1, entonces $i \preceq j$ en $P_1 + P_2$,

(ii) si $i, j \in [n_2]$ y $i \preceq j$ en P_2, entonces $i \preceq j$ en $P_1 + P_2$,

(iii) si $i \in P_1$ y $j \in P_2$, entonces $i \preceq j$ en $P_1 + P_2$.

En este caso, la suma ordinal de posets si es asociativa, pero en general no es conmutativa.

Ejemplo 3.1.10. Sean P_1 y P_2, como en el ejemplo 3.1.8. En la siguiente figura podemos ver la suma ordinal de los posets P_1 y P_2, dados por sus respectivos diagramas de Hasse.



Debemos mencionar, que si bien $P_1 \oplus P_2$ y $P_1 + P_2$ son posets sobre el conjunto $[n_1] \cup [n_2]$, considerando la unión disjunta, podemos considerarlos como posets sobre $[n]$, donde $n = n_1 + n_2$, identificando $[n_1]$ con los primeros n_1 elementos de $[n]$ y a $[n_2]$ con el resto de elementos consecutivamente. A partir de ahora, consideraremos estos posets con esa identificación.

Observación 3.1.11. Es interesante notar que todo poset jerárquico se puede descomponer como la suma ordinal de anticadenas.

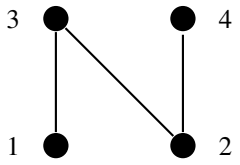
$$\mathbb{H}(n;n_1,\ldots,n_k) = \bigoplus_{i=1}^{k} \mathbb{H}(n_i;n_i).$$

Por ejemplo, el poset $\mathbb{H}(5;2,3) = \mathbb{H}(2;2) \oplus \mathbb{H}(3;3)$.

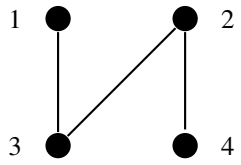
Definición 3.1.12. Sean $P = ([n], \preceq_P)$ un poset, definimos el **poset dual** $P^{\perp}$, como el orden parcial sobre $[n]$ dado por la relación:

$$i \preceq_{P^{\perp}} j \iff j \preceq_P i.$$

Ejemplo 3.1.13. En el siguiente gráfico podemos ver los diagramas de Hasse del Poset P, dado por las relaciones $1 \preceq 3$, $2 \preceq 3$, $2 \preceq 4$ y de su poset dual $P^{\perp}$ dado por las relaciones $3 \preceq 1$, $3 \preceq 2$, $2 \preceq 4$.



P



$P^{\perp}$

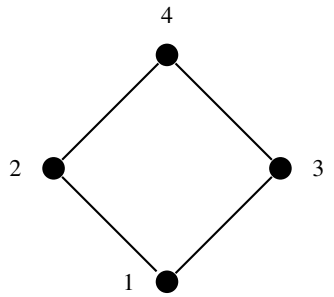
Definición 3.1.14. Una permutación π de $[n]$ es un **automorfismo** del poset $P = ([n], \preceq_P)$ si la acción de π preserva las relaciones de orden del poset, es decir si

$$i \preceq_P j \iff \phi(i) \preceq_Q \phi(j) \quad \text{para todo } i, j \in [n].$$

Denotamos por $Aut(P)$ al grupo de automorfismos del poset P. Notar que dos posets isomorfos siempre pueden representarse por el mismo diagrama de Hasse. Un poset $P = ([n], \preceq_P)$ se dice **autodual** si es isomorfo a su poset dual $P^{\perp}$, es decir, si existe una permutación de $[n]$ tal que

$$i \preceq_P j \iff \pi(i) \preceq_{P^{\perp}} \pi(j) \quad \text{para todo } i, j \in [n].$$

Ejemplo 3.1.15. Sea P el poset dado por las relaciones $1 \preceq 2$, $1 \preceq 3$, $2 \preceq 4$, $3 \preceq 4$ y sea $\pi = (14)$ la transposición que intercambia el 1 con el 4. Entonces se puede ver que P es autodual.



P

3.2. Propiedades métricas de los P-espacios.

Uno de los aspectos básicos en la teoría de códigos es el hecho que, dado un código lineal $\mathcal{C} \subseteq \mathbb{F}_q^n$, existe un código *equivalente* $\mathcal{C}'$ que tiene una matriz generadora en forma *standard*. Para obtener esa matriz necesitamos realizar operaciones básicas sobre filas a la matriz generadora de $\mathcal{C}$ para obtener una matriz escalón reducida por filas, seguido de una permutación de columnas. Debemos remarcar que las operaciones por filas preservan el código, solo dan otra base del mismo, mientras que las permutaciones de columnas, siendo simetrías del espacio con respecto a la métrica de Hamming, dan códigos equivalentes (no necesariamente iguales).

P-equivalencia

Consideremos el espacio $(\mathbb{F}_q^n, d_P)$. Un mapa $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ se dice **P-isometría** si

$$d_P(T(u), T(v)) = d_P(u, v)$$

para todo $u, v \in \mathbb{F}_q^n$.

Denotemos por $\mathrm{GL}_P(\mathbb{F}_q)$ el grupo de isometrías lineales del P-espacio, i.e.,

$$\mathrm{GL}_P(\mathbb{F}_q) := \{T : \mathbb{F}_q^n \to \mathbb{F}_q^n : T \text{ es una } P\text{-isometría lineal}\}.$$

Dos códigos lineales $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^n$ se dicen P-**equivalentes** si existe $T \in \mathrm{GL}_P(\mathbb{F}_q)$ tal que $T(\mathcal{C}) = \mathcal{C}'$. Esta definición coincide con la equivalencia usual de códigos en el espacio de Hamming. Observemos que dos códigos P-equivalentes son, geométricamente hablando, indistinguibles.

Invariantes

Muchas propiedades importantes de códigos estan determinadas por invariantes de la métrica. Por ejemplo, la capacidad correctora de un código está determinada por el radio de empaquetamiento, el

cual, puede (o no) estar determinado por la distancia mínima.

Dado que la distancia d_P sólo asume valores en $[n]\cup\{0\}$, para $u\in\mathbb{F}_q^n$ y $r\in[n]$, sean

$$B(u,r)=\{v\in\mathbb{F}_q^n : d_P(u,v)\leq r\} \qquad \text{y} \qquad S(u,r)=\{v\in\mathbb{F}_q^n : d_P(u,v)=r\}$$

la *bola* y la *esfera* de radio r y centro u, respectivamente Si $\mathcal{S}$ es un subconjunto de $\mathbb{F}_q^n$, entonces:

(i) La **distancia mínima** de $\mathcal{S}$ es la mínima distancia entre dos elementos de $\mathcal{S}$, i.e.,

$$d_P(\mathcal{S})=\text{mín}\{d_P(x,y) : x,y\in\mathcal{S}, x\neq y\}.$$

(ii) El **radio de empaquetamiento** de $\mathcal{S}$ es el entero positivo más grande $\mathcal{P}_P(\mathcal{S})$ tal que las bolas de radio $\mathcal{P}_P(\mathcal{S})$ centradas en los elementos de $\mathcal{S}$ son disjuntas dos a dos, i.e.,

$$\mathcal{P}_P(S)=\text{máx}\{i\in\mathbb{Z} \ : \ B(u,i)\cap B(v,i)=\emptyset, \ \forall\, u,v\in\mathcal{S} \text{ con } u\neq v\}.$$

(iii) El **radio de cubrimiento** de $\mathcal{S}$ es el mínimo entero positivo $\mathrm{C}_{ov,P}(\mathcal{S})$ tal que las bolas de radio $\mathrm{C}_{ov,P}(\mathcal{S})$ centradas en los elementos de $\mathcal{S}$ cubren $\mathbb{F}_q^n$, i.e.,

$$\mathrm{C}_{ov,P}(\mathcal{S})=\text{mín}\left\{i\in\mathbb{Z} \ : \ \mathbb{F}_q^n=\bigcup_{u\in\mathcal{S}}B(u,i)\right\}.$$

(iv) El **radio de Chebyshev** de $\mathcal{S}$ es el mínimo entero positivo $\mathcal{R}_P(\mathcal{S})$ tal que existe una bola centrada en el vector $u\in\mathbb{F}_q^n$ con radio $\mathcal{R}_P(\mathcal{S})$ que contiene a $\mathcal{S}$, i.e.,

$$\mathcal{R}_P(\mathcal{S})=\text{mín}\{i\in\mathbb{Z} \ : \ \mathcal{S}\subseteq B(u,i) \text{ para algún } u\in\mathbb{F}_q^n\}.$$

Un vector u alcanzando este mínimo se dice **centro de Chebyshev** $\mathcal{S}$.

Si no se presenta ninguna confusión, podemos omitir el índice P y escribir sólo $d(\mathcal{S}),\mathcal{P}(\mathcal{S}),C_{ov}(\mathcal{S})$ y $\mathcal{R}(\mathcal{S})$ para la distancia mínima y los radios de empaquetamiento, cubrimiento y de Chebyshev, respectivamente. En [35], los autores dieron una fórmula explícita para la distancia mínima y para el radio de empaquetamiento.

3.3. Grupo de simetrías de métricas poset

En esta sección nos dedicaremos a estudiar los grupos de simetrías de métricas poset. Más específicamente, en el caso de posets jerárquicos podremos dar explícitamente una descripción de tales grupos, generalizando resultados previos de otros autores.

En [51], Panek, Firer et al. calcularon el grupo de isometrías lineales para una métrica poset. En [34], lograron calcular el grupo de simetrías de los espacios de Rosenbloom-Tsfasman.

El siguiente resultado nos permitirá relacionar el grupo de simetrías de la suma ordinal de dos posets con los grupos de simetrías de cada uno de ellos, obteniendo una especie de recursión que facilitará su cálculo. Para ello necesitaremos el siguiente resultado. Para simplificar la notación, dado un poset P en $[n]$, denotaremos por $\mathcal{G}_P$ al grafo de distancias asociado $\mathcal{G}(\mathbb{F}_q^n, d_P)$.

Lema 3.3.1. *Sea $P = P_1 \oplus P_2$ un poset en $[n]$, con P_1 y P_2 posets en $[n_1]$ y $[n_2]$ respectivamente. Entonces, el grafo de distancias asociado $\mathcal{G}_P$ se descompone como la unión de dos grafos de la siguiente forma*

$$\mathcal{G}_P = q^{n_2}\mathcal{G}_{P_1} \cup \mathcal{G}_{P_2}[K^c_{q^{n_1}}],$$

donde $K^c_{q^{n_1}}$ es el grafo con q^{n_1} vértices y ninguna arista.

Demostración. Sean $(x,y),(x',y') \in \mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2}$, entonces tenemos que

$$d_P((x,y),(x',y')) = w_P((x-x',y-y')) = \begin{cases} w_{P_1}(x-x') & \text{si } y = y', \\ n_1 + w_{P_2}(y-y') & \text{si } y \neq y'. \end{cases}$$

Es decir que se cumple la siguiente condición

$$d_P((x,y),(x',y')) \leq n_1 \quad \Longleftrightarrow \quad y = y',$$

por lo tanto, podemos separar el grafo $\mathcal{G}_P$ en dos partes, una cuyas aristas sean las distancias menores o iguales a n_1 y el resto. Claramente, en el primer caso tenemos q^{n_1} (una por cada clase de $\mathbb{F}_q^n/\mathbb{F}_q^{n_1}$) copias del grafo $\mathcal{G}_{P_1}$. En el otro caso, tenemos que si $d_P((x,y),(x',y')) > n_1$, entonces

$$d_P((x,y),(x',y')) = d_P((z,y),(x',y'))$$

para todo $z \in \mathbb{F}_q^{n_1}$. Es decir, el grafo es de la forma $\mathcal{G}_{P_2}[K^c_{q^{n_1}}]$, como queríamos ver. □

Teorema 3.3.2. *Si $P = P_1 \oplus P_2$ un poset en $[n]$, con P_1 y P_2 posets en $[n_1]$ y $[n_2]$ respectivamente, entonces*

$$\Gamma(\mathbb{F}_q^n, d_P) \simeq \Gamma(\mathbb{F}_q^{n_1}, d_{P_1}) \wr \Gamma(\mathbb{F}_q^{n_2}, d_{P_2}).$$

Demostración. Sean $G_1 = \Gamma(\mathbb{F}_q^{n_1}, d_{P_1})$ y $G_2 = \Gamma(\mathbb{F}_q^{n_2}, d_{P_2})$, $X = \mathbb{F}_q^{n_1}$, $Y = \mathbb{F}_q^{n_2}$. Si $\sigma \in G_1^Y$, definimos la función $\phi_\sigma : X \times Y \to X \times Y$ como $\phi_\sigma(x,y) = (\sigma_y(x), y)$. Veamos que $\phi_\sigma \in \Gamma$. Tenemos

$$\begin{aligned} d_P(\phi_\sigma(x_1,y_1), \phi_\sigma(x_2,y_2)) &= d_P((\sigma_{y_1}(x_1), y_1), (\sigma_{y_2}(x_2), y_2)) \\ &= w_P((\sigma_{y_1}(x_1), y_1) - (\sigma_{y_2}(x_2), y_2)) \\ &= w_P((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2), y_1 - y_2)). \end{aligned}$$

Caso $y_1 = y_2$:

$$\begin{aligned} w_P((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2), y_1 - y_2)) &= w_P((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2), 0)) \\ &= |\langle supp((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2), 0))\rangle_P| \\ &= |\langle supp((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2)))\rangle_{P_1}| \\ &= d_{P_1}((\sigma_{y_1}(x_1), \sigma_{y_2}(x_2))) \\ &= d_{P_1}((x_1, x_2)) \\ &= w_{P_1}(x_1 - x_2) \\ &= w_P(x_1 - x_2, 0)) \\ &= w_P((x_1 - x_2, y_1 - y_2)) \\ &= d_P((x_1, y_1), (x_2, y_2)). \end{aligned}$$

Caso $y_1 \neq y_2$:

$$\begin{aligned} w_P((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2), y_1 - y_2)) &= w_P((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2), y_1 - y_2)) \\ &= |\langle supp((\sigma_{y_1}(x_1) - \sigma_{y_2}(x_2), y_1 - y_2))\rangle_P| \\ &= n_1 + |\langle supp(y_1 - y_2)\rangle_{P_2}| \\ &= |\langle supp(x_1 - x_2, y_1 - y_2))\rangle_P| \\ &= d_P((x_1, y_1), (x_2, y_2)). \end{aligned}$$

Sea $\tau \in G_2$, definimos $\varphi_\tau : X \times Y \to X \times Y$ por $\varphi_\tau(x, y) = (x, \tau(y))$. Veamos que $\tau \in \Gamma$. Tenemos

$$\begin{aligned} d_P(\varphi_\tau(x_1, y_1), \varphi_\tau(x_2, y_2)) &= d_P((x_1, \tau(y_1)), (x_2, \tau(y_2))) \\ &= w_P((x_1, \tau(y_1)) - (x_2, \tau(y_2))) \\ &= w_P((x_1 - x_2, \tau(y_1) - \tau(y_2))). \end{aligned}$$

Caso $y_1 = y_2$:

$$\begin{aligned} w_P((x_1 - x_2, \tau(y_1) - \tau(y_2))) &= w_P((x_1 - x_2, 0)) \\ &= w_P((x_1 - x_2, y_1 - y_2)) \\ &= d_P((x_1, y_1), (x_2, y_2)). \end{aligned}$$

Caso $y_1 \neq y_2$:

$$w_P((x_1 - x_2, \tau(y_1) - \tau(y_2))) = n_1 + w_{P_2}(\tau(y_1) - \tau(y_2)).$$

Esto nos dice que $G_1^Y, G_2 \subset \Gamma$.

Ahora consideremos el grafo de distancias asociado a la métrica d_p. Es claro que podemos descomponerlo en la unión de dos grafos $\mathcal{G}_1$ y $\mathcal{G}_2$, correspondientes a las aristas de peso menor o igual que n_1, y mayor que n_1, respectivamente. Claramente $\mathcal{G}_1$ es la unión disjunta de q^{n_2} copias (una por cada coclase de $\mathbb{F}_q^n/\mathbb{F}_q^{n_1}$) del grafo asociado a $(F_q^{n_1}, d_{p_1})$, por lo tanto

$$Aut(\mathcal{G}_1) = G_1 \wr \mathbb{S}_Y.$$

Por otro lado, $\mathcal{G}_2 = \mathcal{G}_{P_2}[K^c_{q^{n_1}}]$, donde $\mathcal{G}_{P_2}$ es el grafo asociado a la distancia $(F_q^{n_2}, d_{p_2})$, entonces

$$Aut(\mathcal{G}_2) = \mathbb{S}_X \wr G_2.$$

Ahora, para finalizar, tenemos que

$$Aut(\mathcal{G}_P) = Aut(\mathcal{G}_{P_1}) \cap Aut(\mathcal{G}_{P_2}) = G_1^Y \rtimes G_2$$

como queríamos ver y la demostración está completa.

□

El Teorema anterior nos permite calcular el grupo de simtrías de un espacio jerárquico.

Teorema 3.3.3. *Sea $P = \mathbb{H}(n; n_1, \ldots, n_k)$ un poset jerárquico, entonces se tiene que*

$$\Gamma(\mathbb{F}_q^n, d_P) \simeq ((\mathbb{S}_q \wr \mathbb{S}_{n_1}) \wr \cdots \wr (\mathbb{S}_q \wr \mathbb{S}_{n_k})).$$

Cuando el poset es una cadena, es decir en el caso de la métrica RT, podemos dar explícitamente el grupo de simetrías. Este resultado coincide con los obtenidos previamente en [34, Cor. 3.1] y [50, Cor. 3.3].

Corolario 3.3.4. *Sea $P = \mathbb{H}(n; 1, \ldots, 1)$ un poset cadena, entonces se tiene que*

$$\Gamma(\mathbb{F}_q^n, d_P) \simeq (\underbrace{\mathbb{S}_q \wr \cdots \wr \mathbb{S}_q}_{n}).$$

Demostración. Como el poset P es jerárquico, por el Teorema 3.3.3 tenemos que el grupo de simetrías es $\Gamma(\mathbb{F}_q^n, d_P) \simeq (\mathbb{S}_q \wr \mathbb{S}_1) \wr \cdots \wr (\mathbb{S}_q \wr \mathbb{S}_1)$. Usando que $\mathbb{S}_1 = id$, se tiene que $\mathbb{S}_n \wr \mathbb{S}_1 = \mathbb{S}_n$, de donde se tiene el resultado buscado. □

Ejemplo 3.3.5. Consideremos de nuevo el poset jerárquico $P = \mathbb{H}(8; 3, 2, 3)$, dado por la siguiente figura. El teorema anterior nos dice que el grupo de simetrías de la métrica inducida por ese poset es

$$\Gamma(\mathbb{F}_q^8, d_P) \simeq \big((\mathbb{S}_q \wr \mathbb{S}_3) \wr (\mathbb{S}_q \wr \mathbb{S}_2)\big) \wr (\mathbb{S}_q \wr \mathbb{S}_3).$$

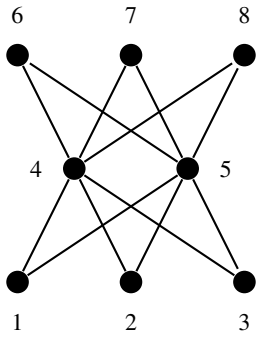


Figura 3.1: $\mathbb{H}(8;3,2,3)$

El cardinal de este grupo es

$$|\Gamma(\mathbb{F}_q^8, d_P)| = ((q!^3 3!)^{q^2} q!^2 2)^{q^3} q!^3 3!$$

Por ejemplo, si $q = 2$ se tiene

$$|\Gamma(\mathbb{F}_2^8, d_P)| = ((2^3 6)^4 8)^3 48 = 2^{16} 3^4 = 3.676.258.543.978.604.182.634.496$$

lo cual muestra lo grande que son estos grupos de simetrías.

3.4. Métricas poset con pesos

Sea (G, d_{Ham}) el espacio métrico de Hamming. Podemos extender la métrica de Hamming a una métrica en G^n de la siguiente forma

$$d(x,y) := \sum_{k=1}^{n} 2^k \, d_{Ham}(x_k, y_k) \tag{3.2}$$

con $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in G^n$.

Notemos que dados $x, y \in G^n$, $w(x) = w(y)$ si y sólo si $supp(x) = supp(y)$, es decir si para cada $i = 0, \ldots, n$ se tiene que $w_{Ham}(x_i) = w_{Ham}(y_i)$. Es decir, la partición inducida por (G^n, d) es de la forma

$$\mathcal{P} = \left\{ P_{i_1} \times \cdots \times P_{i_n} \ : \ P_{i_j} \in \mathcal{P}_{Ham}, j = 1, \ldots, n \right\}.$$

Por lo tanto (G^n, d) es la métrica producto de n copias de (G, d_{Ham}) (ver 2.2.17).

Ejemplo 3.4.1. En particular, tomando $n = 2$, obtenemos una distancia en $\mathbb{Z}_2 \times \mathbb{Z}_2$ dada por los siguientes pesos

$$w(x) = \begin{cases} 0 & \text{si } x = (0,0), \\ 1 & \text{si } x = (1,0), \\ 2 & \text{si } x = (0,1), \\ 3 & \text{si } x = (1,1), \end{cases}$$

La métrica descripta anteriormente es un ejemplo de *métrica de Hamming con pesos* ([4]), que a su vez puede verse como un caso particular de *métricas poset con pesos* ([26]), como veremos a continuación.

Sea $(P, \preceq)$ un conjunto parcialmente ordenado y sea π una función de P en $\mathbb{N}$. Diremos que $(P, \preceq, \pi)$ es un **poset con π-pesos**, al cual denotaremos por P_π. El P_π-**peso** de $x \in G^n$ esta definido por

$$w_{P_\pi}(x) = \sum_{i \in \langle x \rangle_P} \pi(i).$$

La P_π-**distancia** de vectores $x, y \in G^n$ está definida como

$$d_{P_\pi}(x,y) = w_{P_\pi}(x-y).$$

Notemos que cuando la función de pesos $\pi : P \to \mathbb{N}$ esta dada por $\pi(i) = 1$ para todo i en P, tenemos que

$$d_{P_\pi}(x,y) = d_P(x,y),$$

es decir coincide con la definición de métrica poset.

Lema 3.4.2. *Si P_π es un poset con pesos, entonces la P_π-distancia d_{P_π} es una métrica en G^n.*

En particular, la métrica producto definida en (3.2) se puede obtener tomando el poset anticadena y la función

$$\begin{aligned} \pi : P &\to \mathbb{N} \\ k &\mapsto 2^k. \end{aligned}$$

Supongamos ahora que queremos extender de la misma forma una métrica (G,d), a una métrica (G^n, d^n_{Prod}). Sea

$$r = \max_{x \in G} \{w(x)\} + 1,$$

entonces tomando la función

$$\begin{aligned} \pi : P &\to \mathbb{N} \\ k &\mapsto r^k, \end{aligned}$$

definimos la métrica producto,

$$d^n_{Prod}(x,y) := d_{P_\pi} = \sum_{k=1}^{n} r^k \, d(x_k - y_k) \qquad x,y \in G^n.$$

Ejemplo 3.4.3. Consideremos es espacio métrico $(\mathbb{Z}_2, d_{Ham})$, en este caso tenemos que $r = 2$, por lo tanto podemos definir la métrica producto

$$d^n_{Prod}(x,y) := d_{P_\pi} = \sum_{k=1}^{n} 2^k \, d_{Ham}(x_k - y_k) \qquad x,y \in G^n.$$

En particular, tomando $n = 2$, obtenemos una distancia dada por los siguientes pesos

$$w^n_{Prod}(x) = \begin{cases} 0 & \text{si } x = (0,0), \\ 1 & \text{si } x = (1,0), \\ 2 & \text{si } x = (0,1), \\ 3 & \text{si } x = (1,1), \end{cases}$$

Recordemos que en el caso de métricas inducidas por un poset jerárquico $\mathbb{H}(n; n_1, \ldots, n_k)$ se correspondían con los esquemas de asociación de la forma $H(n_1, q) \wr \cdots \wr H(n_k, q)$. Ahora, consideramos $\mathbb{H}(n, n_1, \ldots, n_k)$ como un poset con pesos, dándole a cada nivel la función peso correspondiente para obtener la métrica de *Hamming con pesos*. Por lo tanto, la métrica obtenida será de la forma

$$d^{n_1}_{Prod} \wr \cdots \wr d^{n_k}_{Prod}.$$

Capítulo 4

Dualidad e identidades de MacWilliams

En la teoría de códigos, uno de los resultados más importantes es la identidad de MacWilliams, que relaciona el enumerador de peso de un código con el enumerador de pesos de su código dual. Esta identidad, originalmente para códigos lineales con las distancia de Hamming, fue generalizada para esquemas de asociación por Delsarte [14]. En este capítulo utilizando la dualidad de esquemas de asociación, definiremos la dualidad de métricas para obtener las correspondientes identidades de MacWilliams. En particular, para el caso de métricas poset daremos otra descripción de esta identidad.

4.1. Dualidad

En esta sección G será un grupo abeliano finito (en caso de no aclararse lo contrario). Definiremos el concepto de dualidad de una métrica, que está relacionado con la existencia de una identidad de MacWillians que relaciona el enumerador de peso de un código con el enumerador de peso del código dual, análogo al caso de la distancia de Hamming. Daremos condiciones para determinar cuándo una métrica es reflexiva o autodual.

El grupo de caracteres de G se define como $\widehat{G} := Hom(G, \mathbb{C}^*)$ con la operación

$$(\chi_1 + \chi_2)(g) := \chi_1(g)\chi_2(g) \quad \forall \chi_i \in \widehat{G}, g \in G.$$

Seguiremos el trabajo de Zinoviev y Ericson en [68].

Es bien sabido que G y $\widehat{G}$ son isomorfos (no canónicamente), y en particular $|G| = |\widehat{G}|$. Los grupos G y $\widehat{\widehat{G}}$ son naturalmente isomorfos mediante el mapeo que lleva el elemento $g \in G$ al carácter de $\hat{G}$ que envía $\chi \in \hat{G}$ a $\chi(g)$. Por lo tanto $g(\chi) = \chi(g)$. Esto nos sugiere utilizar la notación $\langle \chi, g \rangle := \chi(g)$,

y por lo tanto tenemos las identidades

$$\begin{aligned}\langle \chi, g\rangle &= \langle g, \chi\rangle \\ \langle \chi, g_1 + g_2\rangle &= \langle \chi, g_1\rangle\langle \chi, g_2\rangle \\ \langle \chi_1 + \chi_2, g\rangle &= \langle \chi_1, g\rangle\langle \chi_2, g\rangle.\end{aligned}$$

Definición 4.1.1. Sea G un grupo abeliano. Un **código aditivo** $\mathcal{C}$ de longitud n sobre R es un subgrupo $\mathcal{C} \in G^n$.

Definición 4.1.2. Sea $\mathcal{C} \leq G$ un código aditivo, i.e. un subgrupo de G, definimos el **código dual** $\mathcal{C}^\perp \leq \widehat{G}$ como sigue

$$\mathcal{C}^\perp = \{\chi \in \widehat{G} : \langle \chi, h\rangle = 1,\ \forall h \in \mathcal{C}\}.$$

Es fácil ver que $\mathcal{C}^\perp \simeq \widehat{G/\mathcal{C}}$, y por lo tanto $|\mathcal{C}^\perp||\mathcal{C}| = |G|$, y más aún $(\mathcal{C}^\perp)^\perp = \mathcal{C}$ para todo $\mathcal{C} \leq G$.

Sea V un espacio vectorial complejo y sea $f : G \to V$. La **transformada de Fourier** de f es

$$\begin{aligned}\widehat{f} : \widehat{G} &\longrightarrow V \\ \chi &\longmapsto \sum_{g\in G} \langle \chi, g\rangle f(g)\end{aligned}$$

La transformada de Fourier es invertible, y con la identificación canónica de G y $\widehat{\widehat{G}}$, se tiene que

$$\widehat{\widehat{f}}(g) = |G| f(-g).$$

La función f y su transformada de Fourier satisfacen la siguiente fórmula (sumatoria de Poisson)

$$\sum_{x\in\mathcal{C}^\perp} \widehat{f}(\chi) = |\mathcal{C}^\perp| \sum_{h\in\mathcal{C}} f(h),$$

para todo código $\mathcal{C} \in G$.

Definición 4.1.3. Denotemos por $\mathbb{C}^G$ al espacio vectorial de todas las funciones $G \to \mathbb{C}$. Dada una partición $\mathcal{P}$ de G, definimos

$$L(\mathcal{P}) = \{f \in \mathbb{C}^G \ :\ f(x) = \sum_{i=0}^{n} f_i \mathbf{1}_{P_i}\},$$

donde $\mathbf{1}_{P_i}$ es la función característica del conjunto P_i.

Definición 4.1.4. Sea $\mathcal{P} = P_1|\cdots|P_M$ una partición de G. La **partición dual** de $\mathcal{P}$, denotada $\widehat{\mathcal{P}}$, es la

partición de $\widehat{G}$ definida por la relación de equivalencia:

$$\chi \sim_{\widehat{\mathcal{P}}} \chi' \iff \sum_{g\in P_m} \langle \chi, g\rangle = \sum_{g\in P_m} \langle \chi', g\rangle \quad \chi,\chi' \in \widehat{G}, m = 1,\dots,M.$$

Sea $\widehat{\mathcal{P}} = Q_1|\cdots|Q_L$, definimos los **coeficientes de Krawtchouk generalizados**:

$$K_{\ell,m} = \sum_{g\in P_m} \langle \chi, g\rangle$$

donde χ es cualquier elemento en Q_l.

La matriz $K = (K_{l,m}) \in \mathbb{C}^{N\times M}$ es la **matriz de Krawtchouk generalizada** de $(\mathcal{P}, \widehat{\mathcal{P}})$. La partición $\mathcal{P}$ se dice **Fourier reflexiva**, o simplemente **reflexiva**, si $\widehat{\widehat{\mathcal{P}}} = \mathcal{P}$. Identificando los grupos isomorfos G y $\hat{G}$ podríamos tener que $\widehat{\mathcal{P}} = \mathcal{P}$, en este caso diremos que $\mathcal{P}$ es autodual (con respecto al isomorfismo dado entre G y $\hat{G}$).

Observación 4.1.5. Es importante notar que en el caso que $\mathcal{P}$ sea una partición de Schur, entonces la definición previa coincide con la definición de anillos de Schur duales (ver (1.15)).

En [21], Gluesing-Luerssen caracterizó la reflexividad de una partición. El resultado nos permite decir que si la partición dual $\widehat{\mathcal{P}}$ tiene el mismo número de bloques que $\mathcal{P}$, entonces $\mathcal{P}$ es reflexiva.

Teorema 4.1.6. *Se tiene que* $|\mathcal{P}| \le |\widehat{\mathcal{P}}|$ *y* $\widehat{\widehat{\mathcal{P}}} \le \mathcal{P}$. *Más aún,* $\mathcal{P}$ *es reflexiva si y sólo si* $|\mathcal{P}| = |\widehat{\mathcal{P}}|$.

Las particiones reflexivas están relacionadas directamente con los esquemas de asociación. De hecho, con el resultado anterior es posible demostrar que la partición $\mathcal{P}$ es reflexiva si y sólo si la partición $\mathcal{R} = R_1|R_2|\cdots|R_M$ de $G\times G$ definida por $(x,y) \in R_m \Leftrightarrow x - y \in P_m$ es un esquema de asociación abeliano. En el estudio de esquemas de asociación, esto ya fue establecido en [48, Cor. 4.51] asi también como en [68, Thm. 1] y se remonta a [49, Sec. 2.6.1].

Ahora veremos que si $\mathcal{P} = P_1|\dots|P_M$ es una partición unitaria simétrica de G entonces $\widehat{\mathcal{P}}$ es una partición unitaria simétrica de $\widehat{G}$.

El conjunto $\{\chi_e\}$, donde χ_e es el cáracter trivial, siempre es un bloque de $\widehat{\mathcal{P}}$. Supongamos que $\chi \in \widehat{G}$ pertenece a la misma partición que $\{\chi_e\}$, es decir que

$$\sum_{g\in P_m} \langle \chi_e, g\rangle = \sum_{g\in P_m} \langle \chi, g\rangle \qquad \chi \in \widehat{G}, m = 1,\dots,M,$$

entonces se tiene que

$$\sum_{m=1}^{M}\sum_{g\in P_m}\langle\chi_e,g\rangle=\sum_{m=1}^{M}\sum_{g\in P_m}\langle\chi,g\rangle$$

$$\sum_{g\in G}\langle\chi_e,g\rangle=\sum_{g\in G}\langle\chi,g\rangle,$$

y esta igualdad sólo se da si $\chi=\chi_e$. Esto prueba que $\widehat{\mathcal{P}}$ es unitaria. Ahora, como $\mathcal{P}$ es simétrica, tenemos que

$$\sum_{g\in P_m}\langle\chi,g\rangle=\sum_{g\in P_m}\langle\chi,-g\rangle=\sum_{g\in P_m}\langle\chi^{-1},g\rangle,$$

es decir que χ y χ^{-1} están en el mismo bloque de $\widehat{\mathcal{P}}$, por lo tanto, $\widehat{\mathcal{P}}$ es una partición simétrica de $\widehat{G}$. Estas observaciones nos permiten dar la siguiente definición.

Definición 4.1.7. Dado $d\in\mathcal{M}(G)/\sim_{\mathcal{P}}$ definimos la **métrica dual** $d^*\in\mathcal{M}(\widehat{G})/\sim_{\mathcal{P}}$ como la métrica inducida en $\widehat{G}$ por la partición dual de $\mathcal{P}(G,d)$. En general dado un isomorfismo entre G y $\widehat{G}$, podemos considerar la métrica d^* como una métrica sobre G. Dadas dos métricas $d_1,d_2\in\mathcal{M}(G)/\sim_{\mathcal{P}}$, diremos que d_2 es una **métrica dual** de d_1 si $d_2=d_1^*$ vía algún isomorfismo entre G. y $\widehat{G}$. Diremos que la métrica d es **reflexiva** o **autodual** si la partición asociada es reflexiva o autodual, respectivamente.

En particular para toda métrica schuriana, su partición induce un esquema de asociación, por lo tanto es reflexiva.

Definición 4.1.8. Definimos la **tabla de caracteres** de un espacio métrico (G,d) como la matriz de Krawtchouk generalizada $K=(K_{l,m})\in\mathbb{C}^{N\times M}$. Claramente si la matriz es cuadrada entonces d es reflexiva, y si es autodual, se tiene que $K^2=|G|\mathbf{I}_m$.

Observación 4.1.9. Si (G,d) es una métrica de Schur, entonces la tabla de caracteres de la métrica es cuadrada y coincide con la tabla de caracteres del esquema de asociación inducido por las distancias.

La matriz $K=(K_{\ell,m})\in\mathbb{C}^{N\times M}$ puede obtenerse en función de la *tabla de caracteres* de G, como veremos en el siguiente ejemplo.

Ejemplo 4.1.10. Consideremos el grupo $G=\mathbb{Z}_6$ con la métrica d dada por la partición simétrica $\mathcal{P}=0|1,5|2,3,4$. Sea $\omega=e^{\frac{2\pi i}{6}}$ la raiz sexta primitiva de la unidad. Entonces, tenemos la siguiente tabla de caracteres de $\mathbb{Z}_6$.

Tabla de caracteres de $\mathbb{Z}_6$

	0	1	2	3	4	5
χ_0	1	1	1	1	1	1
χ_1	1	ω	ω^2	-1	ω^4	ω^5
χ_2	1	ω^2	ω^4	1	ω^2	ω^4
χ_3	1	-1	1	-1	1	-1
χ_4	1	ω^4	ω^2	1	ω^4	ω^2
χ_5	1	ω^5	ω^4	-1	ω^2	ω^1

Ahora procedemos a sumar las columnas correspondientes a la partición $\mathcal{P}$, es decir, la columna 1 con la 5 y las columnas $2,3$ y 4, obteniendo:

$$\begin{array}{c} \\ \chi_0 \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \end{array} \begin{array}{c} \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & -1 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & -1 & \omega^2 & \omega^1 \end{pmatrix} \end{array} \Longrightarrow \begin{array}{c} \\ \chi_0 \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \end{array} \begin{array}{c} \begin{array}{ccc} \{0\} & \{1,5\} & \{2,3,4\} \end{array} \\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \\ 1 & -2 & 1 \\ 1 & -1 & 0 \\ 1 & 1 & -2 \end{pmatrix} \end{array}$$

Luego, descartamos las filas repetidas, y agrupamos los caracteres que corresponden a la misma clase de la partición dual de $\mathcal{P}$, obteniendo así la tabla de caracteres de la métrica:

	{0}	{1,5}	{2,3,4}
$\{\chi_0\}$	1	2	3
$\{\chi_1,\chi_5\}$	1	1	-2
$\{\chi_2,\chi_4\}$	1	-1	0
$\{\chi_3\}$	1	-2	1

Podemos ver que la métrica d no es reflexiva, pues el cardinal de la partición dual es mayor que el

cardinal de la partición $\mathcal{P}$.. Identificando $\mathbb{Z}_6$ con $\widehat{\mathbb{Z}}_6$ mediante el isomorfismo inducido por $1 \mapsto \chi_1$, vemos que la métrica dual d^* es de tipo Lee.

La dualidad de anillos de Schur ofrece una gran cantidad de resultados que podemos utilizar en el estudio de dualidad de métricas. Como consecuencia directa del Lema 1.5.12 tenemos el siguiente resultado.

Proposición 4.1.11. *Sea G un grupo abeliano, y sea $d \in \mathcal{M}(G)$ una métrica schuriana. Entonces*

(i) Si d es orbital, entonces es autodual.

(ii) Si $d = d_1 \times d_2$ entonces $d^* = d_1^* \times d_2^*$.

(iii) Si $d = d_1 \wr d_2$ entonces $d^* = d_2^* \wr d_1^*$.

(iv) Si $d = d_1 \wedge_K d_2$ entonces $d^* = d_2^* \wedge_{K^\perp} d_1^*$.

Ejemplo 4.1.12. La métrica de Lee d_{Lee} sobre $\mathbb{Z}_m$ es orbital, pues la partición esta dada por la acción del automorfismo de inversión $i : G \to G$. Entonces por el Teorema anterior, d_{Lee} es autodual.

Definición 4.1.13. Sea G un grupo abeliano, y sea $H \leq G$ un subgrupo. Definimos la métrica asociada al subgrupo H, que denotaremos d_H, dada por la partición

$$H \setminus \{e\}, G \setminus H.$$

Esta resulta ser una métrica de Schur, pues la partición es un caso particular de un anillo de Schur reticular, dada por la cadena de subgrupos $\{e\} < H < G$.

Proposición 4.1.14. *Sea $H \leq G$, con G un grupo abeliano, entonces las métricas $d_H^* = d_{H^\perp}$.*

Demostración. Sean $1_e, 1_{H\setminus\{e\}}, 1_{G\setminus H}$ las funciones características de $\{e\}, H \setminus \{e\}$ y $G \setminus H$, respectivamente. Entonces, tenemos que

$$\widehat{1}_e(\chi) = \chi(e) = 1. \tag{4.1}$$

$$\widehat{1}_{H\setminus\{e\}}(\chi) = \sum_{h\in H-e} \chi(h) = \begin{cases} |H|-1 & \text{si } \chi \in H^\perp, \\ -1 & \text{si } \chi \notin H^\perp, \end{cases} \tag{4.2}$$

y

$$\widehat{1}_{G\setminus H}(\chi) = \sum_{g\in G-H} \chi(g) = \begin{cases} |G|-|H| & \text{si } \chi = \mathbf{1}_G, \\ -|H| & \text{si } \chi \in H^\perp - \mathbf{1}_G, \\ 0 & \text{si } \chi \notin H^\perp. \end{cases} \tag{4.3}$$

Por lo tanto, la partición asociada a d_H^* es $1_G \mid H^\perp - 1_G \mid \hat{G} - H^\perp$, como se queria ver. □

En particular, si $H \simeq H^\perp$, se tiene que d_H es autodual.

4.2. Identidades de MacWilliams

En esta sección nos dedicaremos a estudiar las identidades de MacWilliams para enumeradores de pesos de códigos en G y sus códigos duales en $\hat{G}$. Estos resultados generales pueden ser encontrados en [48, Thm. 4.72, Prop. 5.42], donde Camion los derivó con la ayuda de esquemas de asociación, y en [20, p. 94] done Forney los obtuvo para subgrupos discretos de grupos abelianos localmente compactos. En [49, p. 88] Delsarte ya conocía la conexión entre los esquemas de asociación abelianos y las identidades de MacWilliams. En la forma de (4.2.2) abajo y para el caso especial de particiones autoduales (i. e., $\mathcal{P} = \widehat{\mathcal{P}}$ identificando G y $\hat{G}$), la identidad fue establecida por Zinoviev-Ericson en [64, Teo 1].

Sean $\mathcal{P} = P_1 \mid \cdots \mid P_M$ y $\mathcal{Q} = Q_1 \mid \cdots \mid Q_L$ particiones de G y $\hat{G}$, respectivamente, tales que $\mathcal{P} = \widehat{\mathcal{Q}}$ Sea $K = (K_{m,\ell}) \in \mathbb{C}^{M\times L}$ la matriz de Krawtchouk de $(\mathcal{Q},\mathcal{P})$. Para un código $\mathcal{C} \leq G$ y su dual $\mathcal{C}^\perp \leq \hat{G}$ definimos los **enumeradores de partición** $\mathrm{PE}_{\mathcal{P},\mathcal{C}} \in \mathbb{C}[X_1,\ldots,X_M]$ y $\mathrm{PE}_{\mathcal{Q},\mathcal{C}^\perp} \in \mathbb{C}[Y_1,\ldots,Y_L]$ de la siguiente manera

$$\mathrm{PE}_{\mathcal{P},\mathcal{C}} = \sum_{m=1}^{M} A_m X_m, \quad \mathrm{PE}_{\mathcal{Q},\mathcal{C}^\perp} = \sum_{\ell=1}^{L} B_\ell Y_\ell, \tag{4.4}$$

donde $A_m = |\mathcal{C} \cap P_m|$ y $B_\ell = |\mathcal{C}^\perp \cap Q_\ell|$. Estos enumeradores tienen la información de la cantidad de palabras del código contenidas en cada bloque de la partición.

Dados $\mathcal{P} = P_1 \mid \cdots \mid P_M$ una partición de G y $g \in G$, definimos el **índice** $i(g)$, como el único número tal que $0 \leq i(g) \leq M$ y $g \in P_i$.

Definición 4.2.1. Dados un espacio métrico (G,d) y un codigo $\mathcal{C} \leq G$, el **enumerador de peso** de $\mathcal{C}$ es

$$W_{C,d}(\vec{X}) = \sum_{g\in C} X_{i(g)},$$

donde $\vec{X} = (X_0, X_1, \ldots, X_M)$.

Teorema 4.2.2 (MacWilliams)**.** *Sea (G,d) un espacio métrica y sea d^* la métrica dual, $\mathcal{C} \leq G$ un código y P la tabla de caracteres del esquema de asociación correspondiente a (G,d), entonces*

$$W_{\mathcal{C},d}(\vec{Y}) = \frac{1}{|\mathcal{C}^\perp|} W_{\mathcal{C}^\perp,d^*}(P\vec{X}).$$

Ejemplo 4.2.3. Sea $\mathcal{C}$ un código en $(\mathbb{Z}_5, d_{Lee})$. Sabemos que la métrica de Lee d_{Lee} es autodual,

entonces para usar el Teorema anterior, calculamos la tabla de caracteres:

$$P = \begin{pmatrix} 1 & 2 & 2 \\ 1 & \varphi - 1 & -\varphi \\ 1 & -\varphi & \varphi - 1 \end{pmatrix}.$$

por lo tanto la identidad de MacWilliams correspondiente es

$$W_{\mathcal{C}^\perp}(x,y,z) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x+2y+2z, x+(\varphi-1)y-\varphi z, x+-\varphi y+(\varphi-1)z),$$

donde $\varphi = \frac{1+\sqrt{5}}{2}$.

4.2.1. Dualidad sobre anillos

Ahora podemos considerar códigos sobre R^n, con R un anillo finito, es decir, tomamos un anillo en lugar de un grupo G.

Definición 4.2.4. Sea R un anillo finito. Un **código lineal** a izquierda (a derecha) $\mathcal{C}$ de longitud n sobre R es un R-submódulo a izquierda (a derecha) $\mathcal{C} \in R^n$.

Los resultados vistos anteriormente sobre dualidad de códigos aditivos se pueden generalizar a códigos lineales sobre anillos, pues claramente todo código lineal de R^n es un código aditivo del grupo base de R. El único inconveniente es que en R^n tenemos definido un producto punto canónico

$$x \cdot y = \sum_i^n x_i y_i \quad \text{para todo} x, y \in R^n,$$

el cual nos permite, dado un código $\mathcal{C} \in R^n$, definir un código dual

$$\mathcal{C}^{\perp\perp} := \{v \in R^n : v \cdot a = 0 \text{ para todo } a \in \mathcal{C}\},$$

el cual es el utilizado tradicionalmente en el estudio de códigos sobre $\mathbb{F}_q$ y sobre anillos finitos en general. Ahora que los resultados anteriores sobre dualidad e identidades de MacWilliams sigan valiendo, deberíamos identificar de alguna forma el código dual (con respecto al grupo de caracteres) con el código dual con respecto al producto punto. Esta situación se da exactamente cuando R es un anillo de Frobenius. A continuación daremos la definición y el resultado que nos permite relacionar las dos definiciones de códigos duales. Sólo daremos una mínima reseña sobre esto, para mas información sobre la importancia de los anillos de Frobenius en la Teoría de Códigos, recomendamos leer el trabajo de Jay Wood [66].

Sea R un anillo conmutativo finito con identidad.Su grupo de unidades se denota $\mathcal{U}(R)$. El grupo de caracteres de $(R,+)$ puede ser dotado de una estructura de R-módulo mediante la multiplicación escalar definida por $r\chi(a) := \chi(ra)$, y llamamos a $\widehat{R}$ el **módulo de caracteres** de R.

Mientras que los grupos aditivos de R y $\widehat{R}$ son isomorfos, esto no es necesariamente cierto para el caso de los R-módulos R y $\widehat{R}$. Estos últimos son isomorfos si y sólo si R es un anillo de Frobenius. En la teoría de anillos, los anillos de Frobenius se definen comúnmente a través de su sócalo (ver [29, Def. 16.14]). Sin embargo, para anillos conmutativos finitos, se sigue (ver Hirano [24, Thm. 1] y Honold [25, p. 409]) que es equivalente a la definición que daremos a continuación.

Definición 4.2.5. Un anillo conmutativo finito R se dice de **Frobenius** si existe un caracter $\chi \in \widehat{R}$ tal que $\alpha : R \longrightarrow \widehat{R},\ r \longmapsto r\chi$ es un isomorfismo de R-módulos. Cualquier carácter χ con esta propiedad se dice **carácter generador** de R.

Obviamente, dos caracteres generadores χ, χ' difieren en una unidad, i.e., $\chi' = u\chi$ para algún $u \in \mathcal{U}(R)$.

Muchos ejemplos clásicos de anillos conmutativos son anillos de Frobenius. A continuación veremos algunos ejemplos. Mas detalles se pueden encontrar en [65, Exam. 4.4].

Ejemplo 4.2.6.

(i) El anillo de enteros $\mathbb{Z}_n$, donde $n \in \mathbb{N}$, es un anillo de Frobenius. Un carácter generador esta dado por $\chi(g) := \zeta^g$ para todo $g \in \mathbb{Z}_n$, donde $\zeta \in \mathbb{C}$ es una raíz n-ésima primitiva de la unidad. Cada carácter esta dado por $a\chi(g) = \chi(ag) = \zeta^{ag}$ para algún $a \in \mathbb{Z}_n$.

(ii) Todo cuerpo finito $\mathbb{F}_q$ con $q = p^r$ es un anillo de Frobenius. Sea $Tr : \mathbb{F}_q \to \mathbb{F}_p$ la función traza, entonces un carácter generador es de la forma $\chi(k) := e^{2\pi i Tr(k)/p}$ para todo $k \in \mathbb{F}_p$.

(iii) Anillos de cadena finitos, anillos de grupo finitos sobre un anillo de Frobenius, producto directo de anillos de Frobenius y anillos de Galois son también anillos de Frobenius.

(iv) El anillo $R = \mathbb{F}_2[x,y]/(x^2, y^2, xy)$ es un anillo local que no es Frobenius; ver [11, Ex. 3.2].

El siguiente resultado se puede encontrar en [21, Thm. 5.4]. Para la parte (ii) también se puede encontrar en [65, Thm. 7.7]

Teorema 4.2.7. *Sea R un anillo de Frobenius finito y conmutativo, y sea χ un carácter generador de R. Sean $v, a \in R^n$, denotamos por $v \cdot a := \sum_{i=1}^{n} v_i a_i$ el producto interno canónico. Más aún, para $v \in R^n$ definimos el carácter $\chi_v \in \widehat{R^n}$ via $\chi_v(a) = \chi(v \cdot a) = \langle \chi, v \cdot a \rangle$ para todo $a \in R^n$. Entonces tenemos lo siguiente:*

(i) El mapa $\alpha :\ R^n \longrightarrow \widehat{R^n}, \quad y \longmapsto \chi_y$ es un isomorfismo de R-módulos.

(ii) Para un código $\mathcal{C} \subseteq R^n$ definimos el código dual con respecto al producto interno canónico como $\mathcal{C}^{\perp\!\!\!\perp} := \{v \in R^n \mid v \cdot a = 0$ para todo $a \in \mathcal{C}\}$. Entonces el código aditivo dual $(\mathcal{C}, +)$ y el dual con respecto al producto interno coinciden; precisamente

$$\alpha(\mathcal{C}^{\perp\!\!\!\perp}) = \mathcal{C}^{\perp} = \{\psi \in \widehat{R^n} : \langle \psi, a \rangle = 1 \text{ for all } a \in \mathcal{C}\}.$$

Este teorema nos dice que al trabajar códigos sobre R^n, con R un anillo de Frobenius, los resultados de dualidad e identidades de MacWilliams pueden utilizarse para relacionar el enumerador de peso de un código $\mathcal{C} \subseteq R^n$ con el enumerador de peso de su código dual con respecto al producto punto, así como lo hacíamos en el caso aditivo.

Observación 4.2.8. Para todo anillo de Frobenius R y todo código $\mathcal{C} \subseteq R^n$, se tiene que $(\mathcal{C}^{\perp\!\!\!\perp})^{\perp\!\!\!\perp} = \mathcal{C}$, por lo tanto, $|\mathcal{C}||(\mathcal{C}^{\perp\!\!\!\perp})| = |R^n|$. Si $n = 1$, entonces $\mathcal{C} \subseteq R$ es un ideal en R, y la identidad $\mathcal{C}^{\perp\!\!\!\perp\,\perp\!\!\!\perp} = \mathcal{C}$ se conoce como la propiedad del doble anulador (ver [29, Thm. 15.1]). Esta propiedad no se cumple en general si R no es un anillo de Frobenius. Por ejemplo, consideremos el ideal $\mathcal{C} = (x)$ en el anillo $R = \mathbb{F}_2[x,y]/(x^2, y^2, xy)$. En este caso, $(x)^{\perp\!\!\!\perp} = (x,y)$ y $(x)^{\perp\!\!\!\perp\,\perp\!\!\!\perp} = (x,y) \neq (x)$ (por lo tanto R no puede ser un anillo de Fobenius).

4.2.2. Identidades de MacWilliams para métricas poset

En [27], [45], los autores estudiaron la existencia de identidades de MacWilliams para métricas poset y probaron que ser un poset jerárquico es una condición necesaria y suficiente para que la métrica inducida admita una identidad de MacWilliams. Además, dieron fórmulas explicitas para las automatrices de los esquemas de asociación dados por esas métricas. Utilizando esos resultados en los posets anticadenas y cadenas, se pueden obtener la identidades de MacWilliams para la métrica de Hamming y la métrica de Rosenbloom-Tasfaman, obtenida en [58].

Definición 4.2.9. Dado un $P = ([n], \preceq)$, se dice que **admite un esquema de asociación**, si el par $(\mathbb{F}_q^n, \mathcal{R}_{d_P})$ es un esquema de asociación, donde

$$\mathcal{R}_{d_P} = \left\{(x,y) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \,:\, d_p(x,y) = i\right\}.$$

En la terminología utilizada en esta tesis, esto nos dice que P admite un esquema de asociación si y sólo si la métrica d_P es una métrica de Schur. Ahora podemos considerar la siguiente caracterización de posets jerárquicos.

Teorema 4.2.10 ([37, Thm. 3]). *Sea $P = ([n], \preceq)$ un poset y se $(\mathbb{F}_q, d_P)$ el espacio poset correspondiente. Entonces son equivalentes:*

(i) P es un poset jerárquico.

(ii) P admite un esquema de asociación.

Es decir que una métrica poset d_P sobre $\mathbb{F}_q^n$ es una métrica de Schur y sólo si P es un poset jerárquico. Esta es una de las razones por las cuales la familia de posets jerárquicos parecen ser mas importantes. El siguiente teorema nos permitirá determinar la métrica dual d_p^*, en el caso que P sea un poset jerárquico.

Teorema 4.2.11 ([46, Thm. 3.8]). *Sea P un poset jerárquico. Entonces, $(\mathbb{F}_q^n, \mathcal{R}_{P^\perp})$ y $(\widehat{\mathbb{F}_q^n}, \mathcal{R}_P^*)$ son isomorfos como esquemas de asociación.*

Es decir que los anillos de Schur correspondientes son isomorfos, por lo tanto, se tiene el siguiente resultado.

Teorema 4.2.12. *Sea P un poset jerárquico. Entonces, d_P y $d_{P^\perp}$ son duales.*

Ahora que sabemos esto, pasaremos a determinar explícitamente la identidad de MacWilliams, utilizando los resultados de las secciones anteriores. Supongamos que $P = P_1 \oplus P_2$ es un poset sobre $[n]$, y P_1, P_2 son posets sobre $[n_1]$ y $[n_2]$ respectivamente, con $n = n_1 + n_2$. Consideremos el espacio métrico $(\mathbb{F}_q^n, d_p)$. Ahora sea χ un carácter de $\mathbb{F}_q^n \simeq \mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2}$, y sea $u = (x,y) \in \mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2}$, entonces se tiene que

$$\chi(u) = \chi_{n_1}(x)\chi_{n_2}(y), \tag{4.5}$$

donde χ_{n_1}, χ_{n_2} son caracteres de $\mathbb{F}_q^{n_1}$ y $\mathbb{F}_q^{n_2}$ respectivamente. De lo cual deducimos que si $u = (x,y) \in \mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2}$, y $\chi \in (\mathbb{F}_q^{n_1})^\perp$, entonces tenemos que

$$\chi(x,y) = \chi_{n_2}(y). \tag{4.6}$$

Además, si $y = (0, \ldots, 0)$ tenemos que

$$\chi(x,y) = \chi_{n_1}(x). \tag{4.7}$$

Comenzamos ahora con la tabla de caracteres de $\mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2}$, la cual es de la forma:

$$
(\mathbb{F}_q^{n_1})^{\perp}
\begin{cases}
\overbrace{}^{\mathbb{F}_q^{n_1}} & & & & & & & \\
1 & 1 & \cdots & 1 & * & * & \cdots & * \\
1 & 1 & \cdots & 1 & * & * & \cdots & * \\
\vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\
1 & 1 & \cdots & 1 & * & * & \cdots & * \\
* & \cdots & \cdots & * & * & * & \cdots & * \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
* & * & * & * & * & * & \cdots & *
\end{cases}
$$

Ahora, debemos sumar las columnas correspondientes a cada bloque de la partición $\mathcal{P}(\mathbb{F}_q^n, d_P)$. Para ello observemos que por (4.5),(4.6) y (4.7) tenemos lo siguiente

$$
\sum_{(x,y)\in P_i} \chi(x,y) = \begin{cases} \displaystyle\sum_{x\,|\,(x,y)\in P_i} \chi_{n_1}(x) & \text{si } y = (0,\ldots,0), \\ q^{n_1} \displaystyle\sum_{y\,|\,(x,y)\in P_i} \chi_{n_2}(y) & \text{si } \chi \in (\mathbb{F}_q^{n_1})^{\perp},\ y \neq (0,\ldots,0), \\ 0 & \text{si } \chi \notin (\mathbb{F}_q^{n_1})^{\perp}\ y \neq (0,\ldots,0). \end{cases} \tag{4.8}
$$

Por lo tanto, obtenemos la siguiente matriz

$$
\begin{pmatrix}
a_1 & a_2 & \cdots & a_k & * & * & \cdots & * \\
a_1 & a_2 & \cdots & a_k & * & * & \cdots & * \\
\vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\
a_1 & a_2 & \cdots & a_k & * & * & \cdots & * \\
* & * & \cdots & * & 0 & 0 & \cdots & 0 \\
\vdots & * & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
* & * & \cdots & * & 0 & 0 & \cdots & 0
\end{pmatrix}
$$

A continuación, debemos eliminar las filas repetidas. Utilizando (4.8) y las tablas de caracteres de

$\mathbb{F}_q^{n_1}$ y $\mathbb{F}_q^{n_2}$, obtenemos

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k & & & & \\ a_1 & a_2 & \cdots & a_k & & \tilde{T}_2 & & \\ \vdots & \vdots & \vdots & \vdots & & & & \\ a_1 & a_2 & \cdots & a_k & & & & \\ & & & & 0 & 0 & \cdots & 0 \\ & \bar{T}_1 & & & \vdots & \vdots & \vdots & \vdots \\ & & & & 0 & 0 & \cdots & 0 \end{pmatrix},$$

donde $\bar{T}_1$ es la matriz obtenida de la tabla de caracteres T_1 de $\mathbb{F}_q^{n_1}$ eliminando la fila correspondiente al bloque $\{\chi_0\}$ (carácter trivial), $\tilde{T}_2$ es la matriz obtenida eliminando la columna correspondiente al bloque $\{0\}$ y $(a_1,\ldots,a_k)$ es la primera fila de la matriz $\bar{T}_1$.

Las consideraciones anteriores nos permiten formular el siguiente teorema que, en el caso particular de que P sea un poset jerárquico, coincide con las identidades de MacWilliams ya conocidas en la literatura, mencionadas por ejemplo en [35].

Teorema 4.2.13. *Sea $P = P_1 \oplus P_2$ un poset, entonces la tabla de caracteres de $(\mathbb{F}_q^n, d_P)$ es de la forma*

$$T = \left(\begin{array}{c:c} A & \tilde{T}_2 \\ \hdashline T_1 & 0 \end{array}\right)$$

donde T_1 es la tabla de caracteres de $(\mathbb{F}_q^{n_1}, d_{P_1})$, y $\hat{T}_2 = q^{n_1} T_2$, donde T_2 es la tabla de caracteres de $(\mathbb{F}_q^{n_2}, d_{P_2})$ con la primer columna eliminada. Además, A es la matriz $n_2 \times (n_1+1)$ cuyas filas $A_{j,*} = (T_1)_{1,*}$, para $1 \leq j \leq n_2$.

En [58], los autores calculan las tablas de caracteres para el caso de los posets cadenas, los cuales compararemos con el método recursivo dado por el teorema anterior.

Ejemplo 4.2.14. Consideremos la métrica RT en $\mathbb{F}_q^n$, es decir, la métrica dada por el poset cadena $P_n = 1 \prec 2 \prec \cdots \prec n$. En particular tenemos que $P_1 = \mathbf{1}$, $P_2 = \mathbf{1} \oplus \mathbf{1}$ y $P_3 = \mathbf{1} \oplus (\mathbf{1} \oplus \mathbf{1}) = (\mathbf{1} \oplus \mathbf{1}) \oplus \mathbf{1}$, donde

1 es el poset que consiste en un único elemento. El teorema anterior nos dice cómo obtener las tablas de caracteres $\theta_1, \theta_2, \theta_3$ correspondientes a cada espacio métrico, utilizando las descomposiciones de los posets.

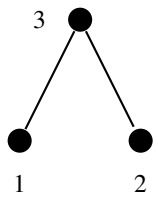
$$\theta_1 = \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \qquad \theta_2 = \left(\begin{array}{cc:c} 1 & q-1 & q(q-1) \\ \hdashline 1 & q-1 & -q \\ \hdashline 1 & -1 & 0 \end{array}\right)$$

$$\theta_3 = \left(\begin{array}{cc:cc} 1 & q-1 & q(q-1) & q^2(q-1) \\ 1 & q-1 & q(q-1) & -q^2 \\ \hdashline 1 & q-1 & -q & 0 \\ \hdashline 1 & -1 & 0 & 0 \end{array}\right) = \left(\begin{array}{ccc:c} 1 & q-1 & q(q-1) & q^2(q-1) \\ \hdashline 1 & q-1 & q(q-1) & -q^2 \\ \hdashline 1 & q-1 & -q & 0 \\ 1 & -1 & 0 & 0 \end{array}\right)$$

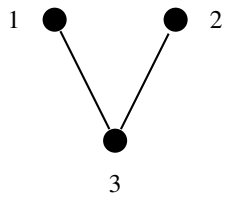
Notemos que en el caso de θ_3 las descomposiciones de la matriz se corresponden con las dos descomposiciones $P_3 = \mathbf{1} \oplus (\mathbf{1} \oplus \mathbf{1}) = (\mathbf{1} \oplus \mathbf{1}) \oplus \mathbf{1}$. Además podemos calcular la matriz θ_3 recursivamente mediante la descomposición $P_3 = (((\mathbf{1}) \oplus \mathbf{1}) \oplus \mathbf{1}))$ y obtener el mismo resultado:

$$\theta_3 = \left(\begin{array}{ccc:c} 1 & q-1 & q(q-1) & q^2(q-1) \\ \hdashline 1 & q-1 & q(q-1) & -q^2 \\ \hdashline 1 & q-1 & -q & 0 \\ \hdashline 1 & -1 & 0 & 0 \end{array}\right).$$

Ejemplo 4.2.15. Consideremos los espacios métricos $(\mathbb{F}_q^3, d_{P_1})$ y $(\mathbb{F}_q^3, d_{P_2})$, dados por los siguientes posets duales.



P_1



P_2

Entonces, utilizando el Teorema 4.2.13, podemos determinar las tablas de caracteres correspon-

dientes que nos permitirán determinar la identidad de Macwilliams.

$$T_1 = \begin{pmatrix} 1 & 2(q-1) & (q-1)^2 & q^2(q-1) \\ 1 & 2(q-1) & (q-1)^2 & -q^2 \\ 1 & q-2 & -(q-1) & 0 \\ 1 & -2 & 1 & 0 \end{pmatrix}, \qquad T_2 = \begin{pmatrix} 1 & q-1 & 2q(q-1) & q(q-1)^2 \\ 1 & q-1 & q(q-2) & -q(q-1) \\ 1 & q-1 & -2q & q \\ 1 & -1 & 0 & 0 \end{pmatrix}.$$

Consideremos el código $\mathcal{C} = \langle (1,1,0) \rangle$. Luego, $\mathcal{C}^\perp = \langle (0,0,1),(1,1,1) \rangle$. Claramente, los enumeradores de pesos de $\mathcal{C}$ con respecto a d_{P_1} y d_{P_2} son los siguientes

$$W_{C,d_{P_1}}(x_0,x_1,x_2,x_3) = x_0 + (q-1)x_2,$$

$$W_{C,d_{P_2}}(x_0,x_1,x_2,x_3) = x_0 + (q-1)x_3,$$

Entonces, usando el Teorema 4.2.2 podemos calcular los enumeradores de peso del código dual $\mathcal{C}^\perp$:

$$\begin{aligned} W_{\mathcal{C}^\perp,d_{P_2}}(x_0,x_1,x_2,x_3) &= \tfrac{1}{|\mathcal{C}|} W_{C,d_{P_1}}(T_2(x_0,x_1,x_2,x_3)^\intercal) \\ &= \tfrac{1}{q}\big(x_0 + (q-1)x_1 + 2q(q-1)x_2 + q(q-1)^2 x_3 \\ &\qquad + (q-1)(x_0 + (q-1)x_1 - 2qx_2 + qx_3)\big) \\ &= \tfrac{1}{q}\big(qx_0 + q(q-1)x_1 + q^2(q-1)x_3\big) \\ &= x_0 + (q-1)x_1 + q(q-1)x_3, \end{aligned}$$

$$\begin{aligned} W_{\mathcal{C}^\perp,d_{P_1}}(x_0,x_1,x_2,x_3) &= \tfrac{1}{|\mathcal{C}|} W_{C,d_{P_2}}(T_1(x_0,x_1,x_2,x_3)^\intercal) \\ &= \tfrac{1}{q}\big(x_0 + 2(q-1)x_1 + (q-1)^2 x_2 + q^2(q-1)x_3 \\ &\qquad + (q-1)(x_0 - 2x_1 + x_2)\big) \\ &= \tfrac{1}{q}\big(qx_0 + q(q-1)x_2 + q^2(q-1)x_3\big) \\ &= x_0 + (q-1)x_2 + q(q-1)x_3. \end{aligned}$$

En particular, para $q = 3$ tenemos

$$\mathcal{C} = \{(0,0,0),(1,1,0),(2,2,0)\},$$

$$\mathcal{C}^\perp = \{(0,0,0),(1,2,0),(2,1,0),(0,0,1),(0,0,2),(1,2,1),(2,1,1),(1,2,2),(2,1,2)\}.$$

Los correspondientes enumeradores de pesos son los siguientes:

$$\begin{aligned}
W_{\mathcal{C},d_{P_1}}(x_0,x_1,x_2,x_3) &= x_0+2x_2,\\
W_{\mathcal{C}^\perp,d_{P_1}}(x_0,x_1,x_2,x_3) &= x_0+2x_2+6x_3,\\
W_{\mathcal{C},d_{P_2}}(x_0,x_1,x_2,x_3) &= x_0+2x_3,\\
W_{\mathcal{C}^\perp,d_{P_2}}(x_0,x_1,x_2,x_3) &= x_0+2x_1+6x_3.
\end{aligned}$$

Capítulo 5

Isometrías

En general, el problema de isometrías consiste en dados grupos G y G', con $|G| = |G'| = n$, determinar si existe alguna métrica que sea invariante por G y G'. En los lenguajes alternativos, encontrar tal métrica es equivalente a encontrar un grupo de simetrías $\Gamma \leq \mathbb{S}_n$, con $G, G' \leq \Gamma$ o encontrar un anillo de Schur (esquema de asociación) sobre G que sea isomorfo a un anillo de Schur (esquema de asociación) sobre G'.En este capítulo discutiremos esta cuestión y obtendremos resultados sobre la existencia de isometrías entre grupos finitos del mismo cardinal, y en particular daremos una isometría explícita de $\mathbb{Z}_q^n$ en el espacio métrico $(\mathbb{F}_q^n, d_{RT})$.

5.1. Isometrías

Un ejemplo trivial es el de la métrica de Hamming, en tal caso se tiene el grupo $\Gamma = \mathbb{S}_n$ que contiene a cualquier grupo de orden n y el anillo de Schur que esta generado por la partición $\mathcal{P} = \{e\}|G \setminus \{e\}$ que es isomorfo al anillo generado por $\mathcal{P} = \{e\}|G' \setminus \{e\}$, para todo grupo G y G' con $|G| = |G'| = n$, es decir que esta es una isometría entre todos los pares de grupos de orden n. Otro ejemplo, quizás el más conocido, es el de la isometría de Gray entre $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$, cuyo grupo de simetrías es $\Gamma \simeq \mathbb{D}_4 \leq \mathbb{S}_4$ y los anillos de Schur correspondientes son los generados por $\mathcal{P} = 0\,|\,1,3\,|\,2$ y $\mathcal{P}' = e \mid (1,0),(0,1) \mid (1,1)$, que son isomorfos.

Mas allá del caso trivial, la pregunta es si dado dos grupos G y G', existe una isometría que no sea la dada por la métrica de Hamming.

Definición 5.1.1. Sean (X_1, d_1) y (X_2, d_2) espacios métricos. Diremos que un mapa $F : X_1 \to X_2$ es una isometría si:

$$d(F(x), F(y)) = d(x, y),\ \forall x, y \in X_1.$$

Diremos que (X_1, d_1) y (X_2, d_2) son **isométricos** si existe una isometría biyectiva $F : X_1 \to X_2$.

Dos espacios métricos son isométricos si y sólo si sus grafos de distancias son isomorfos. Claramente si (G,d) y (G',d') son isométricos entonces $\Gamma(G,d) \simeq \Gamma(G',d')$ y los anillos de Schur correspondientes son isomorfos. Por lo tanto tenemos el siguiente resultado.

Teorema 5.1.2. *Si existe una isometría entre (G_1,d_1) y (G_2,d_2) entonces existe una isometría entre $(G_1,\bar{d_1})$ y $(G_2,\bar{d_2})$, donde $\bar{d_1}$ y $\bar{d_2}$ son las métricas Schurianas representantes de las clases de d_1 y d_2 respectivamente.*

En vistas del resultado anterior y teniendo en cuenta que las métricas schurianas tienen las propiedades más interesantes, consideraremos las isometrías entre esta clase de métricas.

5.2. Isometrías del espacio de Hamming

Debido a la gran importancia y utilidad que mostró el mapa de Gray y el anillo $\mathbb{Z}_4$, en los últimos años ha cobrado gran relevancia el estudio de códigos sobre anillos más generales. Una pregunta natural que surgió fue si existía una generalización del mapa de Gray, que lleve un código lineal sobre $\mathbb{Z}_{p^k}$ a un código sobre $\mathbb{Z}_p$ con propiedades similares. Lamentablemente no se conoce tal generalización, de hecho, en [59] Salagean-Mandache probó que, excepto para el caso conocido $p = k = 2$, no es posible construir una función peso en $\mathbb{Z}_{p^k}$ tal que $\mathbb{Z}_{p^k}$ sea isométrico a $(\mathbb{Z}_p)^k$ con la métrica de Hamming.

En [40] y en [1] los autores tratan el tema de isometrías del espacio de Hamming, con $|X| = m$, no sólo en el caso m primo, y también demuestran que no existe una representación cíclica, es decir una G representación con G un grupo cíclico, del espacio de Hamming, salvo para el caso conocido de la isometría de Gray y los casos triviales $n = 1$. A continuación veremos estos resultados y en algunos casos daremos una prueba alternativa a las encontradas en esos trabajos mencionados.

Lema 5.2.1. *Si G es un grupo finito que contiene a dos subgrupos $H \simeq \mathbb{Z}_q^m$ y $K \simeq \mathbb{Z}_{q^n}$, con $q = p^r$ entonces $|G|$ es divisible por q^{m+n-1}.*

Demostración. Sea P un p-subgrupo de Sylow de G. Como H y K son p-grupos, existen $H', K' \leq P$ conjugados a H y K. Por lo tanto P también contiene subgrupos isomorfos a $\mathbb{Z}_p^m$ y $\mathbb{Z}_{p^n}$. Si probamos que p^{m+n-1} divide a $|P|$ también tendremos que p^{m+n-1} divide a $|P|[G:P] = |G|$. Por lo tanto, es suficiente considerar sólo el caso en que $G = P$ es un p-grupo.

Elegimos y fijamos un grupo P con subgrupos H y K como antes. Entonces

$$|P| \geq |HK| = \frac{|H||K|}{|H \cap K|} \geq \frac{q^m \cdot q^n}{q} = q^{m+n-1}.$$

Como $|P|$ es una potencia de p que es mayor o igual a q^{m+n-1}, $|P|$ is divisible por q^{m+n-1}.(El cálculo depende del hecho que $|H \cap K| = 1$ ó p , pues $H \cap K$ es cíclico de exponente p.) □

Lema 5.2.2. *Si G es un grupo finito que contiene a $H \simeq \mathbb{Z}_m^n$ y a $K \simeq \mathbb{Z}_{m^n}$, con $m \in \mathbb{N}$, entonces $|G|$ es divisible por m^{2n-1}.*

Demostración. Sea $m = p_1^{k_1} \dots p_r^{k_r}$ la descomposición en factores primos de m, y sean $q_i = p_i^r$ Entonces, si G contiene a $H \simeq \mathbb{Z}_m^n$ y a $K \simeq \mathbb{Z}_{m^n}$, también contiene a $H_i \simeq \mathbb{Z}_{q_i}^n$ y a $K_i \simeq \mathbb{Z}_{q_i{}^n}$. Luego, por la proposición anterior $|G|$ es divisible por q_i^{2n-1} para $i = 1, \dots, r$ y por lo tanto $|G|$ es divisible por m^{2n-1}. □

Proposición 5.2.3. *Sea (X^n, d_H) el espacio de Hamming, con $|X| = p$. Si $(p,n) \neq (2,2)$ y $n > 1$, entonces no existe una representación cíclica de (X^n, d_H). En particular, no existe una isometría de $\mathbb{Z}_{p^n}$ en $(\mathbb{Z}_p^n, d_H)$.*

Demostración. El espacio de Hamming tiene una representación cíclica si y solo si el grupo de simetrías tiene un elemento de orden p^n. El grupo de simetrías del espacio de Hamming es $\Gamma(X^n, d_H) \simeq \mathbb{S}_p \wr \mathbb{S}_n$, por lo tanto $|\Gamma(X^n, d_H)| = (p!)^n n!$ Supongamos que existe una representación cíclica. Entonces $\mathbb{Z}_{p^n} \subset \Gamma(X^n, d_H)$, además $\mathbb{Z}_p^n \subset \Gamma(X^n, d_H)$, por lo tanto, por el Lema 5.2.1, p^{2n-1} debe dividir a $|\Gamma(X^n, d_H)| = (p!)^n n!$ Pero tenemos que

$$\begin{aligned} \nu_p((p!)^n n!) &= n\nu_p(p!) + \nu_p(n!) \\ &= n\nu_p(p) + \nu_p(n!) \\ &= n + \nu_p(n!). \end{aligned} \tag{5.1}$$

Ahora, supongamos que $n = n_0 + n_1 p + n_2 p^2 + \ldots + n_r p^r$ es la expansión p-ádica de n, y sea $s_p(n) = n_0 + n_1 + n_2 \ldots + n_r$, entonces la fórmula de Legendre para la valuación p-ádica de $n!$ nos dice que $\nu_p(n!) = \frac{n - s_p(n)}{p-1}$, es decir que tenemos

$$\nu_p((p!)^n n!) = n + \frac{n - s_p(n)}{p-1} \leq n + n - 1 = 2n - 1 \tag{5.2}$$

Mas aún, en (5.2) se da la igualdad si y sólo si $p = 2$ y $n = 2^k$ para algún k. Por lo tanto, sólo resta probar el caso $p = 2$. Alcanzará con ver que si $g \in \Gamma(X^n, d_{Ham}^n) \simeq \mathbb{Z}_2^n \ltimes \mathbb{S}_n$, entonces para $g = (t,s)$, con $t \in \mathbb{Z}_2^n$ y $s \in \mathbb{S}_n$, se tiene que $|g| \leq |t||s| \leq 2e^{\frac{n}{e}}$. En particular si $n > 2$,

$$|g| \leq 2e^{\frac{n}{e}} < 2^n,$$

es decir que no existe ningún elemento de orden 2^n en $\Gamma(X^n, d_{Ham}^n)$. □

Corolario 5.2.4. *No existe una representación cíclica de $(\mathbb{F}_p^n, d_H)$, excepto para $(p,n) = (2,2)$ y los casos triviales $n = 1$.*

Teorema 5.2.5. *Sea (X^n, d_H) un espacio de Hamming, con $|X| = m$. Si $(m,n) \neq (2,2)$ y $n > 1$, entonces no existe una representación cíclica de (X^n, d_H).*

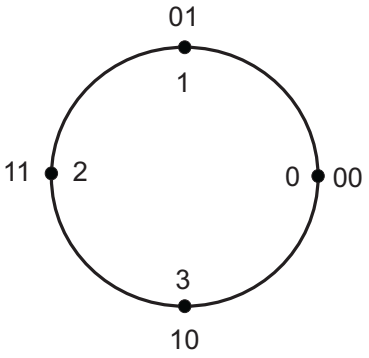
Demostración. El espacio de Hamming tiene una representación cíclica si y solo si el grupo de simetrías tiene un elemento de orden m^n que genere un subgrupo regular. El grupo de simetrías del espacio de Hamming es $\Gamma(X^n, d_H) \simeq \mathbb{S}_m \wr \mathbb{S}_n$. Si $g \in \mathbb{S}_m \wr \mathbb{S}_n$, entonces $|g| \leq mn$, pero si $n > 1$ y $(m,n) \neq (2,2)$, se tiene que $mn < m^n$. □

5.3. Mapas de Gray generalizados

En 1947 Frank Gray inventó el término *código binario reflejado* cuando patentó el sistema de numeración binario en el que dos valores sucesivos difieren solamente en uno de sus dígitos, que luego llevaría su nombre. El código Gray fue diseñado originalmente para prevenir señales espurias de los switches electromecánicos, y actualmente es usado para facilitar la corrección de errores en los sistemas de comunicaciones, entre otras cosas. En [22] se demostró la importancia de este mapeo, al resolver el misterio de la dualidad formal entre las familias de códigos no lineales de Kerdock y Preparata. Esto llevó al intento de generalizar este mapeo a otros espacios de Hamming. En esta sección analizaremos los casos conocidos de estas generalizaciones y daremos una construcción formal que engloba a la mayoría de los casos conocidos.

Definición 5.3.1. El **mapa de Gray** $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$, está definido por

$$\begin{aligned} \phi(0) &\longmapsto 00 \\ \phi(1) &\longmapsto 01 \\ \phi(2) &\longmapsto 11 \\ \phi(3) &\longmapsto 10 \end{aligned}$$



el cual se extiende de manera obvia a un mapa de $\mathbb{Z}_4^n$ a $\mathbb{Z}_2^{2n}$ que también se denotará ϕ.

Ejemplo 5.3.2. Sea $n = 3$, $\mathcal{C} = \{000, 321, 112, 222\}$ entonces tenemos

$$\begin{aligned} \phi(000) &= 000000 & \phi(112) &= 010111 \\ \phi(321) &= 101101 & \phi(222) &= 111111 \end{aligned}$$

Es decir que la imagen de $\mathcal{C}$ bajo el mapa de Gray es

$$\phi(\mathcal{C}) = \{000000, 010111, 101101, 111111\}.$$

En [9], Claude Carlet dió una generalización del mapa de Gray para $\mathbb{Z}_{2^k}$, considerando un espacio de llegada más grande, siendo una isometría no sobreyectiva de $\mathbb{Z}_{2^k}$ a $\mathbb{F}_2^{2^{k-1}}$, la cual probó ser una extensión bastante natural.

Definición 5.3.3. Sea k un entero positivo, $u \in \mathbb{Z}_{2^k}$, y $\sum_{i=1}^{k} u_i 2^{i-1}$ su expansión binaria ($u_i = 0, 1$). La imagen de u bajo el mapa de Gray generalizado Φ, es la siguiente función booleana $\Phi(u)$ en $\mathbb{F}_{2^{k-1}}$

$$\Phi(u) = \left((y_1, \ldots, y_{k-1}) \longmapsto u_k + \sum_{i=1}^{k-1} u_i y_i\right).$$

La Proposición 5.2.3 nos dice que salvo el conocido caso de $\mathbb{Z}_4$ en $(\mathbb{Z}_2 \times \mathbb{Z}_2, d_{Ham}^2)$, no existen isometrías entre $\mathbb{Z}_{p^n}$ en $(\mathbb{Z}_p^n, d_{Ham}^n)$. Básicamente porque en $\Gamma(\mathbb{Z}_p^n, d_{Ham}^n)$ no existe un elemento de orden suficientemente grande para generar $\mathbb{Z}_{p^n}$. Entonces naturalmente surge la pregunta: ¿existe una isometría de $\mathbb{Z}_{p^k}$ en $(\mathbb{Z}_p^n, d_{Ham}^n)$.

Esta situación es conocida. En [9], Carlet definió una isometría de Gray generalizada (y una distancia de Lee generalizada asociada) de $\mathbb{Z}_{2^k}$ en $(\mathbb{Z}_2^{2^{k-1}}, d_{Ham}^{2^{k-1}})$. En [67],Yildiz y Ozgera, buscaron una idea más natural de definir un mapeo de Gray y se obtuvo una isometría de $\mathbb{Z}_{p^k}$ con el **peso de Lee extendido**, en $(\mathbb{Z}_p^{p^{k-1}}, d_{Ham}^{p^{k-1}})$.

$$w_L(x) = \begin{cases} x & \text{si } x \leq p^{k-1}, \\ p^{k-1} & \text{si } p^{k-1} \leq x \leq p^k - p^{k-1}, \\ p^{k-1} - x & \text{si } p^k - p^{k-1} \leq x \leq p^k - 1. \end{cases}$$

dando un mapa de Gray de $\mathbb{Z}_{p^k}$ a $\mathbb{Z}_p^{p^{k-1}}$ más natural, que también se extendieron para anillos de Galois $GR(p^k, m)$.

La descripción de tales isometrías es bastante simple, y a continuación vamos a generalizarlas a isometrías de cualquier grupo cíclico $(\mathbb{Z}_m)$ en $(Soc(\mathbb{Z}_m)^n, d_{Ham}^n)$, donde $Soc(\mathbb{Z}_m)$ es el sócalo de $\mathbb{Z}_m$, i.e. el producto de su subgrupos normales minimales, y $n = [\mathbb{Z}_m : Soc(\mathbb{Z}_m)]$. La isometría está dada explícitamente por el homomorfismo de grupos:

$$\begin{aligned} \mathbb{Z}_m &\xrightarrow{\Phi_L} Soc(\mathbb{Z}_m)^n \ltimes \mathbb{S}_n < \Gamma(Soc(\mathbb{Z}_m)^n, d_{Ham}^n) \\ 1 &\longmapsto ((1,0,0,\ldots,0), (1234\ldots n)) \end{aligned}$$

Notemos que este homomorfismo induce un mapeo inyectivo

$$\mathbb{Z}_m \xrightarrow{\varphi_L} Soc(\mathbb{Z}_m)^n,$$

dado por la proyección en las primeras coordenadas, y que la imagen de $\mathbb{Z}_m$ por Φ_L es un subgrupo de $\Gamma(Soc(\mathbb{Z}_m)^n, d^n_{Ham})$ que actúa regularmente sobre $\varphi_L(\mathbb{Z}_m)$. Es decir que φ_L es una isometría de $(\mathbb{Z}_m, d_L)$ en $(Soc(\mathbb{Z}_m)^n, d^n_{Ham})$.

Ejemplo 5.3.4. Si tenemos el grupo $\mathbb{Z}_{12}$, $Soc(\mathbb{Z}_{12}) \simeq \mathbb{Z}_6$, $n = 2$ y la isometría está dada por el homomorfismo

$$\begin{aligned} \mathbb{Z}_{12} &\xrightarrow{\Phi_L} \mathbb{Z}_6^2 \ltimes \mathbb{S}_2 < \Gamma(\mathbb{Z}_6^2, d^2_{Ham}) \\ 1 &\longmapsto ((1,0),(12)) \end{aligned}$$

Mas explícitamente:

$$\begin{aligned} \mathbb{Z}_{12} &\xrightarrow{\varphi_L} \mathbb{Z}_6^2 \\ 0 &\longmapsto (0,0) \\ 1 &\longmapsto (1,0) \\ 2 &\longmapsto (1,1) \\ 3 &\longmapsto (2,1) \\ 4 &\longmapsto (2,2) \\ 5 &\longmapsto (3,2) \end{aligned} \qquad \begin{aligned} \mathbb{Z}_{12} &\xrightarrow{\varphi_L} \mathbb{Z}_6^2 \\ 6 &\longmapsto (3,3) \\ 7 &\longmapsto (4,3) \\ 8 &\longmapsto (4,4) \\ 9 &\longmapsto (5,4) \\ 10 &\longmapsto (5,5) \\ 11 &\longmapsto (0,5) \end{aligned}$$

Es importante notar que esta isometría no depende estrictamente de la métrica de Hamming en $Soc(\mathbb{Z}_m)^n$, ya que la única condición para que este mapa sea una isometría de $\mathbb{Z}_m$ en $(Soc(\mathbb{Z}_m)^n, d)$ es que

$$Soc(\mathbb{Z}_m)^n \ltimes S_n < \Gamma(Soc(\mathbb{Z}_m)^n, d),$$

regularmente, en particular esto se cumple para toda métrica producto simetrizada $Soc(\mathbb{Z}_m)$ en $(Soc(\mathbb{Z}_m)^n$, de las cuales, la métrica de Hamming es un ejemplo.

Estas isometrías generalizan el mapa de Gray en el siguiente sentido, recordemos que $\mathbb{Z}_4$ es isométrico al espacio $(\mathbb{Z}_2 \times \mathbb{Z}_2, d^2_{Ham})$, es decir que tenemos una isometría de $\mathbb{Z}_4$ en (R^2, d^2_{Ham}), donde R es cualquier anillo con grupo base $\mathbb{Z}_2$, en particular $R = \mathbb{F}_2$. Análogamente, tenemos una isometría de $\mathbb{Z}_{p^k}$ en $(\mathbb{Z}_p^{p^{k-1}}, d^{p^{k-1}}_{Ham})$. Notemos que $\mathbb{Z}_p^{p^{k-1}}$ es el grupo base de $\mathbb{F}_p^{p^{k-1}}$, es decir que tenemos el siguiente resultado.

Teorema 5.3.5. *Sea p primo y $k > 1$, entonces existe una isometría de $\mathbb{Z}_{p^k}$ en $(\mathbb{F}_p^{p^{k-1}}, d_{Ham}^{p^{k-1}})$.*

Más generalmente, se puede usar la misma idea para construir isometrías análogas de la siguiente forma.

Definición 5.3.6. Sea $H < \mathbb{Z}_m$ un subgrupo del grupo cíclico $\mathbb{Z}_m$. Si $H = \langle n \rangle$, con $n = [\mathbb{Z}_m : H]$, tenemos que n es el generador mínimo con respecto al orden natural de $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Entonces definimos el **peso de Lee asociado al subgrupo** H, de la siguiente forma:

$$w_{L,H}(x) = \begin{cases} x & \text{si } x \leq n, \\ n & \text{si } n \leq x \leq m-n, \\ n-x & \text{si } m-n \leq x \leq m-1. \end{cases}$$

Exactamente igual al caso anterior, podemos definir un homomorfismo

$$\begin{aligned} \mathbb{Z}_m &\xrightarrow{\Phi_{L,H}} \ltimes \mathbb{S}_n < \Gamma(H^n, d_{Ham}^n) \\ 1 &\longmapsto ((1,0,0,\ldots,0),(1234\ldots n)), \end{aligned}$$

el cual induce un mapeo de Gray

$$\mathbb{Z}_m \xrightarrow{\varphi_{L,H}} Soc(\mathbb{Z}_m)^n,$$

Teorema 5.3.7. *Sea $H < \mathbb{Z}_m$, con G un grupo cíclico finito, y (H,d) un espacio métrico. Entonces existe una isometría de $(\mathbb{Z}_m, d_{L,H})$ en (H^n, d_{Ham}^n), donde $n = [\mathbb{Z}_m : H]$.*

Para finalizar esta sección veremos un pequeño resumen de algunas de las distintas nociones que se trataron de estudiar para generalizar el mapa de Gray. Quizás el principal es el llamado **peso homogéneo** definido en [12], y que fue aplicado a $\mathbb{Z}_{p^k}$ en la forma

$$w_{hom}(x) \begin{cases} 0 & \text{si } x = 0, \\ p^{k-1} & \text{si } 0 \neq x \in p^{k-1}\mathbb{Z}_{p^k}, \\ (p-1)p^{k-2} & \text{en otro caso.} \end{cases}$$

para el cual también se definió un mapa de Gray, que puede ser visto por ejemplo en [32]. El peso homogéneo posee varios puntos a favor, pero también tiene ciertas desventajas como su definición poco natural, y el hecho de no llevar a la construcción de códigos con gran estructura.

Por otro lado, utilizando códigos sobre anillos con mapas de Gray correspondientes, se han descubierto nuevos códigos lineales. Además de $\mathbb{Z}_4$ también se ha considerado el cuerpo $\mathbb{F}_4$ con un mapa de Gray lineal, pero no ha llevado a la construcción de buenos códigos. Recientemente se ha comenzado a considerar un nuevo anillo, $\mathbb{F}_2+u\mathbb{F}_2$, el cual comparte algunas de las buenas propiedades de $\mathbb{Z}_4$ y de $\mathbb{F}_4$. El conjunto de elementos de $\mathbb{F}_2+u\mathbb{F}_2$ es $\{0,1,u,\overline{u}=u+1\}$. Su tabla de multiplicación coincide con la de $\mathbb{Z}_4$, tomando $\overline{u}=3, u=2$, y su tabla de la adición con la de $\mathbb{F}_4=\{0,1,\beta,\beta^2=\beta+1\}$, reemplazando respectivamente u por β y $\overline{u}$ por β^2. Este anillo admite un mapa de Gray natural de $\mathbb{F}_2+u\mathbb{F}_2$ a $\mathbb{F}_{2^2}$

$$\phi(x+uy)=(y,x+y),$$

donde $x,y\in\mathbb{F}_2$.

En [55], Qian et al. caracterizaron la imagen bajo el mapa de Gray de códigos $(1+u)$-cíclicos y códigos cíclicos sobre el anillos $\mathbb{F}_2+u\mathbb{F}_2$ e investigaron códigos constacíclicos sobre $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ en [56].

En [2], Amarra et al. extendieron los resultados de [55] a códigos sobre $\mathbb{F}_p^k+u\mathbb{F}_p^k$. Recientemente, en [10], Cengellenmis presentó los códigos (u^m-1)-cíclicos sobre $\mathbb{F}_2+u\mathbb{F}_2+\cdots+u^m\mathbb{F}_2$ y generalizó los resultados de [55] y [56]. Actualmente se llevan a cabo investigaciones sobre todos estos anillos, más generalmente considerando el caso $\mathbb{F}_q+u\mathbb{F}_q+\cdots+u^m\mathbb{F}_q$, con $q=p^r$.

5.4. Isometrías de grupos

En secciones anteriores vimos que no es posible construir una isometría de $\mathbb{Z}_{m^n}$ en el espacio de Hamming $(\mathbb{Z}_m^n,d_{Ham}^n)$. Ahora discutiremos el caso mas general, de construir una isometría de $\mathbb{Z}_{m^n}$ en el espacio $(\mathbb{Z}_m^n,d)$ para alguna métrica d distinta a la de Hamming. Mas aún veremos la existencia de isometrías no triviales entre dos grupos del mismo cardinal.

Ejemplo 5.4.1. Supongamos que queremos saber si existen isometrías entre $\mathbb{Z}_2^3$ y $\mathbb{Z}_8$. Observemos las siguientes tablas con las clases de grupos de simetrías de métricas de cada uno de los grupos.

Métricas sobre $\mathbb{Z}_8$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7\}$	$\mathbb{S}_8$
2	$\{0\},\{1,2,3,5,6,7\},\{4\}$	$\mathbb{S}_2\wr\mathbb{S}_4$
3	$\{0\},\{1,3,5,7\},\{2,4,6\}$	$\mathbb{S}_4\wr\mathbb{S}_2$
4	$\{0\},\{1,3,5,7\},\{2,6\},\{4\}$	$\mathbb{D}_4\wr\mathbb{S}_2$
5	$\{0\},\{1,7\},\{2,6\},\{3,5\},\{4\}$	$\mathbb{D}_8$

Métricas sobre $\mathbb{Z}_2^3$

N	Partición	Grupo de Simetrías
1	$\{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$	$\mathbb{S}_8$
2	$\{(0,0,0)\},\{(0,0,1),(1,0,1),(0,1,1),(1,1,1)\}$, $\{(1,0,0),(1,1,0),(0,1,0)\}$	$\mathbb{S}_4 \wr \mathbb{S}_2$
3	$\{(0,0,0)\},\{(0,1,0),(0,1,1),(1,1,0),(1,1,1),(1,0,0),(1,0,1)\}$, $\{(0,0,1)\}$	$\mathbb{S}_2 \wr \mathbb{S}_4$
4	$\{(0,0,0)\},\{(0,1,1)\},\{(1,0,0),(1,0,1),(1,1,1),(1,1,0)\}$, $\{(0,0,1),(0,1,0)\}$	$\mathbb{D}_4 \wr \mathbb{S}_2$
5	$\{(0,0,0)\},\{(0,0,1)\},\{(0,1,0),(0,1,1)\},\{(1,0,0),(1,0,1)\}$, $\{(1,1,0),(1,1,1)\}$	$\mathbb{S}_2 \wr (\mathbb{S}_2 \times \mathbb{S}_2)$
6	$\{(0,0,0)\},\{(0,0,1)\},\{(0,1,0)\},\{(0,1,1)\}$, $\{(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$	$(\mathbb{S}_2 \times \mathbb{S}_2) \wr \mathbb{S}_2$
7	$\{(0,0,0)\},\{(0,0,1),(0,1,1),(0,1,0)\},\{(1,0,0)\}$, $\{(1,0,1),(1,1,1),(1,1,0)\}$	$\mathbb{S}_2 \times \mathbb{S}_4 \simeq \mathbb{S}_2 \wr \mathbb{S}_3$
8	$\{(0,0,0)\},\{(0,0,1)\},\{(0,1,0),(0,1,1)\},\{(1,0,0)\},\{(1,0,1)\}$, $\{(1,1,0),(1,1,1)\}$	$\mathbb{S}_2 \times \mathbb{D}_4$
9	$\{(0,0,0)\},\{(0,0,1)\},\{(0,1,0)\},\{(0,1,1)\},\{(1,0,0)\},\{(1,0,1)\}$, $\{(1,1,0)\},\{(1,1,1)\}$	$\mathbb{S}_2 \times \mathbb{S}_2 \times \mathbb{S}_2$

Podemos ver que los únicos grupos que aparecen en las dos tablas son $\mathbb{S}_8$, $\mathbb{S}_4 \wr \mathbb{S}_2$, $\mathbb{S}_2 \wr \mathbb{S}_4$ y $\mathbb{D}_4 \wr \mathbb{S}_2$. Es decir que tendremos esencialmente 4 tipos de isometrías. Por ejemplo, consideremos el grupo $\mathbb{D}_4 \wr \mathbb{S}_2$, construiremos explícitamente una isometría entre $\mathbb{Z}_8$ y $\mathbb{Z}_2^3$, con la métrica dada por ese grupo de simetrías. Supongamos que tenemos una métrica schuriana $(\mathbb{Z}_8, d)$ cuyo grupo de simetrías es $\mathbb{D}_4 \wr \mathbb{S}_2$, intuitivamente vemos que esta métrica debe ser de la forma

$$d = d_1 \wr d_2,$$

donde d_1 es una métrica sobre $\mathbb{Z}_4 \simeq \{0,2,4,6\} \subseteq \mathbb{Z}_8$ y d_2 es una métrica sobre $\mathbb{Z}_2 \simeq \mathbb{Z}_8/\{0,2,4,6\}$. Ahora, viendo la partición

$$\{0\},\{1,3,5,7\},\{2,6\},\{4\},$$

y sabiendo que el grupo de simetrías de d_1 debe ser isomorfo a $\mathbb{D}_4$, podemos concluir que $d_1 \sim_{\mathcal{P}} d_{Lee}$,

donde d_{Lee} es la métrica de Lee sobre $\mathbb{Z}_4$ y $d_1 \sim_{\mathcal{P}} d_{Ham}$, la métrica de Hamming sobre $\mathbb{Z}_2$. Es decir que tenemos que

$$d = d_{Lee} \wr d_{Ham}.$$

Ahora analizando la métrica sobre $\mathbb{Z}_2^3$, análogamente esta vez tenemos que

$$d = d_{Ham}^2 \wr d_{Ham}.$$

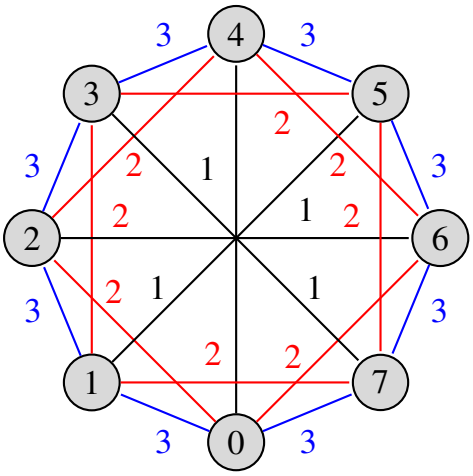
Entonces, ahora podemos usar la isometría de Gray entre $(\mathbb{Z}_4, d_{Lee})$ y $(\mathbb{Z}_2^2, d_{Ham}^2)$ para terminar de construir la isometría buscada. Sea $w : \mathbb{Z}_8 \to \mathbb{R}_{\geq 0}$ definida por

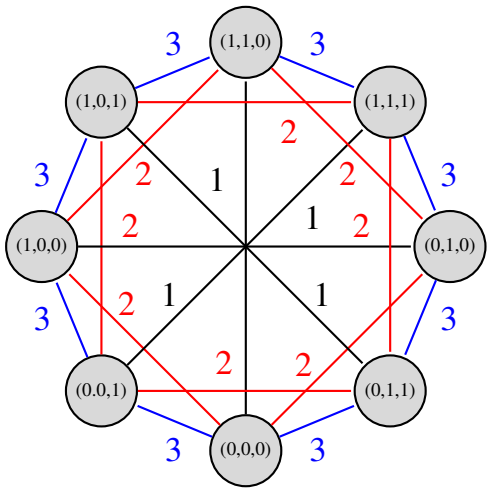
$$w(x) = \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{si } x = 4, \\ 2 & \text{si } x = 2, 6, \\ 3 & \text{si } x = 1, 3, 5, 7. \end{cases}$$

Sea $\phi : \mathbb{Z}_8 \to \mathbb{Z}_2^3$ dada por

$$\begin{array}{ccc} \mathbb{Z}_8 & \xrightarrow{\varphi} & \mathbb{Z}_2^3 \\ 0 & \longmapsto & (0,0,0) \\ 1 & \longmapsto & (0,0,1) \\ 2 & \longmapsto & (1,0,0) \\ 3 & \longmapsto & (1,0,1) \end{array} \qquad \begin{array}{ccc} \mathbb{Z}_8 & \xrightarrow{\varphi} & \mathbb{Z}_2^3 \\ 4 & \longmapsto & (1,1,0) \\ 5 & \longmapsto & (1,1,1) \\ 6 & \longmapsto & (0,1,0) \\ 7 & \longmapsto & (0,1,1). \end{array}$$

Entonces ϕ es una isometría entre $\mathbb{Z}_8$ y $\mathbb{Z}_2^3$, como se puede ver observando los grafos de distancias:





Teorema 5.4.2. *Sean G_1 y G_2 grupos finitos, tales que $|G_1| = |G_2|$, entonces existe una isometría no trivial*

$$(G_1, d_1) \longleftrightarrow (G_2, d_2).$$

Demostración. Sea $m = |G_1| = |G_2|$, y p primo tal que $p|m$. Entonces existen $H_1 < G_1$ y $H_2 < G_1$, con $p = |H_1| = |H_2|$, ahora consideremos los espacios métricos (G_1, d_{H_1}) y (G_2, d_{H_2}), donde d_{H_1} y d_{H_2} son las métricas asociadas a los subgrupos H_1 y H_2 respectivamente, mas explícitamente:

$$d_{H_1}(x,y) = \begin{cases} 0 & \text{si } x = y, \\ 1 & \text{si } x - y \in H_1 \setminus \{0\}, \\ 2 & \text{si } x - y \notin H_1. \end{cases}$$

$$d_{H_2}(x,y) = \begin{cases} 0 & \text{si } x = y, \\ 1 & \text{si } x - y \in H_2 \setminus \{0\}, \\ 2 & \text{si } x - y \notin H_2. \end{cases}$$

Ahora, sean $T_1 = \{g_1, g_2, \ldots, g_{m/p}\}$ y $T_2 = \{g_1', g_2', \ldots, g_{m/p}'\}$ conjuntos de transversales de las clases a derecha de G_i módulo H_i, para $i = 1, 2$. Y sean $\tau : H_1 \to H_2$ y $\rho : T_1 \to T_2$ biyecciones (que existen por ser conjuntos finitos del mismo cardinal). Definimos una biyección $\eta : G_1 \to G_2$ de la forma

$$\begin{array}{ccc} G_1 & \xrightarrow{\eta} & G_2 \\ h + g_i & \longmapsto & \tau(h) + \rho(g_i) \end{array}$$

Si $x - y \in H_1$, entonces x, y pertenecen a la misma coclase de H_1, por lo tanto $\eta(x), \eta(y)$ pertenecen a la misma coclase de H_2, es decir que $\eta(x) - \eta(y) \in H_2$. En resumen tenemos que

$$d_{H_1}(x,y) = 1 \Longleftrightarrow d_{H_2}(\eta(x), \eta(y)) = 1,$$

lo cual sumado que $d_{H_1}(x,y) = 0$ si y sólo si $d_{H_2}(\eta(x), \eta(y)) = 0$, es suficiente para demostrar que η es una isometría

$$(G_1, d_{H_1})(G_2, d_{H_2})$$

□

Observación 5.4.3. Podemos notar que las métricas definidas en el teorema anterior se tiene que

$$\Gamma(G_1, d_{H_1}) \simeq \Gamma(G_2, d_{H_2}) \simeq \mathbb{S}_p \wr \mathbb{S}_{m/p},$$

más aún, no es difícil ver que las métricas d_{H_1} y d_{H_2} son schurianas.

Inmediatamente del Teorema 5.4.2 anterior, tenemos el siguiente resultado

Corolario 5.4.4. *Existe una isometría no trivial entre $\mathbb{Z}_{m^n}$ y $\mathbb{Z}_m^n$, para todo $m, \geq 2$.*

5.5. Isometrías de la métrica RT

En esta sección usaremos los grupos de simetrías calculados en el Capítulo 4 para construir isometrías de los espacios $(\mathbb{F}_q^n, d_P)$, generalizando en cierto sentido la isometría dada por el mapa de Gray, con respecto a métricas poset.

Comenzaremos recordando que el grupo de simetrías de la métrica poset dada por una cadena es de la forma

$$\Gamma(\mathbb{F}_q^n, d_P) \simeq (\mathbb{S}_q \wr \mathbb{S}_q \wr \cdots \wr \mathbb{S}_q).$$

Por lo tanto, para encontrar una isometría de la forma

$$(\mathbb{F}_q^n, d_P) \longleftrightarrow (G, d)$$

primero debemos encontrar una métrica sobre G cuyo grupo de simetrías sea isomorfo a $\Gamma(\mathbb{F}_q^n, d_P)$.

Ejemplo 5.5.1. Recordemos que la métrica RT en $\mathbb{F}_2 \times \mathbb{F}_2$ está dada por

$$w_{RT}(x) = \begin{cases} 0 & \text{si } x = (0,0), \\ 1 & \text{si } x = (1,0), \\ 2 & \text{si } x = (0,1), (1,1). \end{cases}$$

Y su grupo de simetrías es $\Gamma(\mathbb{F}_2^2, d_{RT}) \simeq \mathbb{S}_2 \wr \mathbb{S}_2$.

Ahora consideremos en $\mathbb{Z}_4 = \{0,1,2,3\}$ la métrica dada por

$$w(x) = \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{si } x = 2, \\ 2 & \text{si } x = 1,3. \end{cases}$$

Notemos que el espacio métrico $(\mathbb{Z}_4, d)$ es equivalente al espacio métrico de Lee $(\mathbb{Z}_4, d_{Lee})$, por lo tanto se tiene que $\Gamma(\mathbb{Z}_4, d) \simeq \mathbb{D}_4 \simeq \mathbb{S}_2 \wr \mathbb{S}_2$. Además debemos observar que la partición inducida por la métrica es la misma partición dada por la cadena de subgrupos $\langle 0 \rangle \subset \langle 2 \rangle \subset \mathbb{Z}_4$.

Sea $\phi : \mathbb{Z}_2^2 \to \mathbb{Z}_4$ dada por

$$\begin{array}{ccc} \mathbb{Z}_2^2 & \xrightarrow{\phi} & \mathbb{Z}_4 \\ (0,0) & \longmapsto & 0 \\ (0,1) & \longmapsto & 1 \\ (1,0) & \longmapsto & 2 \\ (1,1) & \longmapsto & 3 \end{array}$$

Entonces, tenemos que $\phi : \mathbb{Z}_2^2 \to \mathbb{Z}_4$ es una isometría entre $(\mathbb{F}_2^2, d_{RT}) \longleftrightarrow (\mathbb{Z}_4, d)$.

El ejemplo anterior nos servirá como base para generalizar la construcción de isometrías para el caso $(\mathbb{F}_q^n, d_{RT})$. Para ello, vamos a construir una métrica sobre $\mathbb{Z}_{q^n}$ tomando una partición en base a una cadena de subgrupos, análogo al ejemplo anterior.

Consideremos la siguiente cadena de subgrupos de G

$$\langle 0 \rangle = B_0 \subset B_1 \subset \cdots \subset B_m = G.$$

Definiremos la siguiente función peso

$$w(x) = \begin{cases} 0 & \text{si } x \in B_0, \\ i & \text{si } x \in B_i \setminus B_{i-1}. \end{cases}$$

Notar que $B_0, B_1 - B_0, \ldots, B_k - B_{m-1}$ forman una partición simétrica de G, por lo que la función peso w está bien definida, e induce naturalmente una función $d : G \times G \to \mathbb{R}_{\geq 0}$

$$d(x,y) = w(x-y) \qquad \forall\, x,y \in G,$$

que claramente es una semimétrica sobre G. Ahora, sólo debemos comprobar que d cumple la desigualdad triangular para concluir que realmente es una función distancia. Supongamos que para algunos elementos $x,y,z \in G$ tenemos que

$$d(x,y) > d(x,z) + d(z,y).$$

Sean $d(x,y) = i$, $d(x,z) = j$ y $d(z,y) = k$, equivalentemente se tiene que

$$x - y \in B_i - B_{i-1} \quad , x - z \in B_j - B_{j-1} \quad , z - y \in B_k - B_{k-1}$$

Podemos asumir que $k \geq j$, por lo tanto $x-y = (x-z)-(y-z) \in B_k - B_{k-1}$, lo cual es absurdo pues $x-y \in B_i - B_{i-1}$ con $B_k \subseteq B_{i-1}$. Es decir que finalmente obtenemos que d es una métrica sobre G.

Métrica q-ádica

En particular, siguiendo el caso anterior, si consideraremos la siguiente cadena de subgrupos

$$\langle 0 \rangle = \langle q^n \rangle \subset \langle q^{n-1} \rangle \subset \langle q^{n-2} \rangle \subset \cdots \subset \langle q^0 \rangle = \mathbb{Z}_{q^n},$$

podemos obtener una métrica sobre $\mathbb{Z}_{q^n}$, la cual definiremos a continuación.

Definición 5.5.2. Definimos el peso q-**ádico** w_q de $x \in \mathbb{Z}_{q^n}$ como:

$$w_q(x) = \begin{cases} 0 & \text{si } x = 0, \\ i & \text{si } x \in \langle q^{i-1} \rangle \setminus \langle q^i \rangle \; i = 1, \ldots, n \; , \end{cases}$$

Naturalmente induce una métrica d_q que llamaremos distancia q-**ádica**:

$$d_q(x,y) = w_q(x-y) = \max_{0 \leq i \leq n} \{ i \; : \; q^{n-i} \mid x-y \}. \tag{5.3}$$

Recordemos la definición de la métrica de Rosenbloom-Tsfasman sobre $\mathbb{F}_q^n$.
Sean $x, y \in \mathbb{F}_q^n$, entonces la métrica d_{RT} esta edefinida por

$$d_{RT}(x,y) = \max_{1 \leq i \leq n} \{ i \; : \; x_i - y_i \neq 0 \}.$$

Si analizamos la partición inducida por esta métrica veremos que está inducida por la cadena

$$\langle 0 \rangle = B'_0 \subset B'_1 \subset \cdots \subset B'_n = \mathbb{F}_q^n,$$

donde $B_i = \{ x \in \mathbb{F}_q^n \; : \; x_i \neq 0, x_j = 0 \; \forall \, i < j \leq n \}$.

Ahora, construiremos explícitamente una isometría utilizando las consideraciones anteriores. Sea $\phi : \mathbb{F}_q^n \to \mathbb{Z}_q^n$ la función

$$\phi(a_1, a_2, \ldots, a_n) \longmapsto a_1 q^{n-1} + a_2 q^{n-2} + \cdots + a_{n-1} q + a_n \pmod{q^n}.$$

Y sea $\phi^{-1} : \mathbb{F}_q^n \to \mathbb{Z}_q^n$ su función inversa dada por la expansión en base q.

$$
\begin{array}{rcl}
0 & \longmapsto & 0000\ldots000 \\
1 & \longmapsto & 0000\ldots001 \\
\vdots & & \vdots \\
q-1 & \longmapsto & 0000\ldots00(q-1) \\
q & \longmapsto & 0000\ldots010 \\
q+1 & \longmapsto & 0000\ldots011 \\
\vdots & & \vdots \\
q^2-1 & \longmapsto & 0000\ldots0(q-1)(q-1) \\
q^2 & \longmapsto & 0000\ldots100 \\
q^2+1 & \longmapsto & 0000\ldots101 \\
\vdots & & \vdots \\
q^n-1 & \longmapsto & (q-1)(q-1)(q-1)(q-1)\ldots(q-1)(q-1)(q-1)
\end{array}
$$

Ahora si consideramos los espacios $(\mathbb{F}_q^n, d_{RT})$ y $(\mathbb{Z}_{q^n}, d_q)$, es claro que $\phi : \mathbb{F}_q^n \to \mathbb{Z}_q^n$ preserva pesos de las palabras. Mas aún, veremos que ϕ preserva distancias, es decir que realmente es una isometría.

Teorema 5.5.3. *Sea $\mathbb{F}_q^n$ con la distancia d_{RT} de Rosenbloom-Tsfasman . Entonces ϕ es una isometría*

$$(\mathbb{F}_q^n, d_{RT}) \longleftrightarrow (\mathbb{Z}_{q^n}, d_q),$$

donde d_q es la distancia q -ádica.

Demostración. Supongamos que $d_{RT}(x,y) = k$, con $x, y \in \mathbb{F}_q^n$, es decir que

$$x_k \neq y_k \quad \text{y} \quad x_i = y_i \quad \text{para todo } i = k+1, \ldots, n. \tag{5.4}$$

Por otro lado,

$$d_q(\phi(x), \phi(y)) = \max_{0 \leq i \leq n} \{ i \ : \ q^{n-i} \ \mid \ \phi^{-1}(x) - \phi^{-1}(y) \},$$

donde, por (5.4) se tiene que

$$\phi(x) - \phi(y) = (x_1 - y_1)q^{n-1} + (x_2 - y_2)q^{n-2} + \cdots + (x_k - y_k)q^{n-k} \pmod{q^n},$$

con $x_k - y_k \neq 0$, es decir que

$$d_q(\phi(x), \phi(y)) = k = d_{RT}(x,y)$$

entonces tenemos que ϕ es una isometría. □

Conclusión

"Cat: Where are you going?
Alice: Which way should I go?
Cat: That depends on where you are going.
Alice: I don't know.
Cat: Then it doesn't matter which way you go".
–Lewis Carrol, Alice in Wonderland

Métricas sobre grupos y anillos

El estudio de métricas sobre grupos y anillos finitos mediante su grupo de simetrías resulta ser una forma general de estudiar propiedades importantes de métricas para la teoría de códigos, en particular la existencia de una identidad de MacWilliams que relacione el enumerador de pesos de un código con el enumerador de pesos de su código dual. También resulta ser de extrema utilidad para considerar la existencia de isometrías de espacios métricos, que en un principio se construían como biyecciones ad hoc, pero gracias a este punto de vista se sabe que tales isometrías estan relacionadas con isomorfismos de grafos (e isomorfismos de los grupos de simetrías).

En particular el Teorema 5.1.2 nos permite restringir la búsqueda de isometrías al caso de métricas Schurianas, lo cual simplifica la tarea, además de fortalecer la idea de que este tipo de métricas son las más adecuadas a considerar en la teoría de códigos pues son la clase de métricas que posee una identidad de MacWilliams. Se logró calcular el grupo de simetrías de un espacio métrico dado por un poset jerárquico, generalizando los resultados conocidos para poset cadenas. También se logró dar una descripción nueva de las identidades de MacWilliams para códigos sobre espacios poset jerárquicos. Así como también se logró establecer nuevos ejemplos de métricas que provienen de esquemas de asociación, utilizando poset con pesos. Y por último, utilizando los cálculos de los grupos de simetrías para construir isometrías entre espacios poset sobre $\mathbb{F}_q^n$ y espacios métricos sobre $\mathbb{Z}_{q^n}$.

Nuevos horizontes

La mayoría de los resultados sobre propiedades de métricas obtenidos previamente pueden ser determinados desde el punto de vista de este trabajo, en muchos casos de forma considerablemente más simple, lo cual nos lleva a pensar que este método es una buena forma de estudiar métricas en el contexto de la teoría de códigos. En este trabajo se determinó cuando una métrica dada posee una identidad de MacWilliams clásica, en el futuro también se puede considerar la idea de si existen otro tipo de identidades que relacionen los enumeradores de pesos de un código y su dual. También se puede trabajar en determinar cuales métricas poseen la *propiedad de extensión*, una pregunta que aún sigue abierta y que esta siendo estudiada actualmente con mucho enfásis. Se pueden intentar calcular los grupos de simetrías para espacios poset en general, no necesariamente jerárquicos. Además, la mayoría de las definiciones y resultados obtenidos en este trabajo pueden ser generalizados a métricas sobre grupos e anillos infinitos, lo cual puede ser de utilidad en otras ramas de la matemática, como la teoría geométrica de grupos y cualquier otra rama que considere métricas, como las métricas p-ádicas.

Apéndice A

Métricas schurianas sobre $\mathbb{Z}_n$

A continuación daremos las tablas de métricas schurianas para grupos cíclicos, con sus correspondientes grupos de simetrías. Notar que cada métrica esta ordenada a continuación de su métrica dual sin una linea horizontal que las separe. En caso contrario significará que es una métrica autodual.

Métrica sobre $\mathbb{Z}_3$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2\}$	$\mathbb{S}_3$

Métricas sobre $\mathbb{Z}_4$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3\}$	$\mathbb{S}_4$
2	$\{0\},\{1,3\},\{2\}$	$\mathbb{D}_4$

Métricas sobre $\mathbb{Z}_5$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4\}$	$\mathbb{S}_5$
2	$\{0\},\{1,4\},\{2,3\}$	$\mathbb{D}_5$

Métricas sobre $\mathbb{Z}_6$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5\}$	$\mathbb{S}_6$
2	$\{0\},\{1,3,5\},\{2,4\}$	$\mathbb{S}_3 \wr \mathbb{S}_2$
3	$\{0\},\{1,2,4,5\},\{3\}$	$\mathbb{S}_2 \wr \mathbb{S}_3$
4	$\{0\},\{1,5\},\{2,4\},\{3\}$	$\mathbb{D}_6$

Métricas sobre $\mathbb{Z}_7$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6\}$	$\mathbb{S}_7$
2	$\{0\},\{1,6\},\{2,5\},\{3,4\}$	$\mathbb{D}_7$

Métricas sobre $\mathbb{Z}_8$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7\}$	$\mathbb{S}_8$
2	$\{0\},\{1,2,3,5,6,7\},\{4\}$	$\mathbb{S}_2 \wr \mathbb{S}_4$
3	$\{0\},\{1,3,5,7\},\{2,4,6\}$	$\mathbb{S}_4 \wr \mathbb{S}_2$
4	$\{0\},\{1,3,5,7\},\{2,6\},\{4\}$	$\mathbb{D}_4 \wr \mathbb{S}_2$
5	$\{0\},\{1,7\},\{2,6\},\{3,5\},\{4\}$	$\mathbb{D}_8$

Métricas sobre $\mathbb{Z}_9$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8\}$	$\mathbb{S}_9$
2	$\{0\},\{1,2,7,8,4,5\},\{3,6\}$	$\mathbb{S}_3 \wr \mathbb{S}_3$
3	$\{0\},\{1,8\},\{2,7\},\{3,6\},\{4,5\}$	$\mathbb{D}_9$

Métricas sobre $\mathbb{Z}_{10}$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9\}$	$\mathbb{S}_{10}$
2	$\{0\},\{1,3,5,7,9\},\{2,4,6,8\}$	$\mathbb{S}_5 \wr \mathbb{S}_2$
3	$\{0\},\{1,2,3,4,6,7,8\},\{5\}$	$\mathbb{S}_2 \wr \mathbb{S}_5$
4	$\{0\},\{1,3,7,9\},\{2,4,6,8\},\{5\}$	$\mathbb{S}_2 \times \mathbb{S}_5$
5	$\{0\},\{1,4,6,9\},\{2,3,7,8\},\{5\}$	$\mathbb{D}_5 \wr \mathbb{S}_2$
6	$\{0\},\{1,3,5,7,9\},\{2,8\},\{4,6\}$	$\mathbb{S}_2 \wr \mathbb{D}_5$
7	$\{0\},\{1,9\},\{2,8\},\{3,7\},\{4,6\},\{5\}$	$\mathbb{D}_{10}$

Métricas sobre $\mathbb{Z}_{11}$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10\}$	$\mathbb{S}_{11}$
2	$\{0\},\{1,10\},\{2,9\},\{3,8\},\{4,7\},\{5,6\}$	$\mathbb{D}_{11}$

Métricas sobre $\mathbb{Z}_{12}$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11\}$	$\mathbb{S}_{12}$
2	$\{0\},\{1,3,5,7,9,11\},\{2,4,6,8,10\}$	$\mathbb{S}_6 \wr \mathbb{S}_2$
3	$\{0\},\{1,2,7,3,8,4,9,5,10,11\},\{6\}$	$\mathbb{S}_2 \wr \mathbb{S}_6$
4	$\{0\},\{1,2,4,7,5,8,10,11\},\{3,6,9\}$	$\mathbb{S}_4 \wr \mathbb{S}_3$
5	$\{0\},\{1,3,9,11,2,5,7,10,6\},\{4,8\}$	$\mathbb{S}_3 \wr \mathbb{S}_4$
6	$\{0\},\{1,2,5,7,11,10\},\{3,6,9\},\{4,8\}$	$\mathbb{S}_3 \times \mathbb{S}_4$
7	$\{0\},\{1,3,5,7,9,11\},\{2,4,8,10\},\{6\}$	$\mathbb{S}_2 \wr \mathbb{S}_3 \wr \mathbb{S}_2$
8	$\{0\},\{1,3,5,7,9,11\},\{2,6,10\},\{4,8\}$	$\mathbb{S}_3 \wr \mathbb{D}_4$
9	$\{0\},\{1,2,4,5,7,8,10,11\},\{3,9\},\{6\}$	$\mathbb{D}_4 \wr \mathbb{S}_3$
10	$\{0\},\{1,5,7,11\},\{2,4,8,10\},\{3,9\},\{6\}$	$\mathbb{S}_2 \wr \mathbb{D}_6$
11	$\{0\},\{1,3,5,7,9,11\},\{2,10\},\{4,8\},\{6\}$	$\mathbb{D}_6 \wr \mathbb{S}_2$
12	$\{0\},\{1,5,7,11\},\{2,10\},\{3,9\},\{4,8\},\{6\}$	$\mathbb{Z}_{12} \rtimes \mathbb{Z}_4 \simeq \mathbb{D}_4 \times \mathbb{S}_3$
13	$\{0\},\{1,11\},\{2,10\},\{3,9\},\{4,8\},\{5,7\},\{6\}$	$\mathbb{D}_{12}$

Métricas sobre $\mathbb{Z}_{13}$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12\}\}$	$\mathbb{S}_{13}$
2	$\{0\},\{1,3,4,9,10,12\},\{2,5,6,7,8,11\}$	$\mathbb{Z}_{13} \rtimes \mathbb{Z}_6$
3	$\{0\},\{1,5,8,12\},\{2,3,10,11\},\{4,6,7,9\}$	$\mathbb{Z}_{13} \rtimes \mathbb{Z}_4$
4	$\{0\},\{1,12\},\{2,10\},\{3,10\},\{4,9\},\{5,8\},\{6,7\}$	$\mathbb{D}_{13}$

Métricas sobre $\mathbb{Z}_{14}$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12,13\}\}$	$\mathbb{S}_{14}$
2	$\{0\},\{1,3,5,7,9,11,13\},\{2,4,6,8,10,12\}$	$\mathbb{S}_7 \wr \mathbb{S}_2$
3	$\{0\},\{1,2,3,4,5,6,8,9,10,11,12,13\},\{7\}$	$\mathbb{S}_2 \wr \mathbb{S}_7$
4	$\{0\},\{1,3,5,9,11,13\},\{2,4,6,8,10,12\},\{7\}$	$\mathbb{S}_2 \times \mathbb{S}_7$
5	$\{0\},\{1,6,8,13\},\{2,5,9,12\},\{3,4,10,11\},\{7\}$	$\mathbb{S}_2 \wr \mathbb{D}_7$
6	$\{0\},\{1,7,9,13,3,5,11\},\{2,12\},\{4,10\},\{6,8\}$	$\mathbb{D}_7 \wr \mathbb{S}_2$
7	$\{0\},\{1,13\},\{2,12\},\{3,11\},\{4,10\},\{5,9\},\{6,8\},\{7\}$	$\mathbb{D}_{14}$

Métricas sobre $\mathbb{Z}_{15}$

N	Partición	Grupo de Simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$	$\mathbb{S}_{15}$
2	$\{0\},\{1,2,4,5,7,8,10,11,13,14\},\{3,6,9,12\}$	$\mathbb{S}_5 \wr \mathbb{S}_3$
3	$\{0\},\{1,2,3,4,6,7,8,9,11,12,13,14\},\{5,10\}$	$\mathbb{S}_3 \wr \mathbb{S}_5$
4	$\{0\},\{1,4,6,9,11,14\},\{2,3,7,8,12,13\},\{5,10\}$	$\mathbb{S}_3 \wr \mathbb{D}_5$
5	$\{0\},\{1,2,4,5,7,8,10,11,13,14\},\{3,12\},\{6,9\}$	$\mathbb{D}_5 \wr \mathbb{S}_3$
6	$\{0\},\{1,2,4,7,8,11,13,14\},\{3,6,9,12\},\{5,10\}$	$\mathbb{D}_5 \times \mathbb{S}_3$
7	$\{0\},\{1,4,11,14\},\{2,7,8,13\},\{3,12\},\{5,10\},\{6,9\}$	$\mathbb{S}_3 \times \mathbb{D}_5$
8	$\{0\},\{1,14\},\{2,13\},\{3,12\},\{4,11\},\{5,10\},\{6,9\},\{7,8\}$	$\mathbb{D}_{15}$

Métricas sobre $\mathbb{Z}_{16}$

N	Partición	G. de simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$	$\mathbb{S}_{16}$
2	$\{0\},\{1,3,5,7,9,11,13,15\},\{2,4,6,8,10,12,14\}$	$\mathbb{S}_8 \wr \mathbb{S}_2$
3	$\{0\},\{1,2,3,4,5,6,7,9,10,11,12,13,14,15\},\{8\}$	$\mathbb{S}_2 \wr \mathbb{S}_8$
4	$\{0\},\{1,2,3,5,6,7,9,10,11,13,14,15,\},\{4,12,8\}$	$\mathbb{S}_4 \wr \mathbb{S}_4$
5	$\{0\},\{1,3,5,7,9,11,13,15\},\{2,6,10,14,4,12\},\{8\}$	$\mathbb{S}_2 \wr \mathbb{S}_4 \wr \mathbb{S}_2$
6	$\{0\},\{1,3,5,7,9,11,13,15\},\{2,6,10,14\},\{4,12,8\}$	$\mathbb{S}_4 \wr \mathbb{D}_4$
7	$\{0\},\{1,2,3,5,6,7,9,10,11,13,14,15\},\{4,12\},\{8\}$	$\mathbb{D}_4 \wr \mathbb{S}_4$
8	$\{0\},\{1,3,5,7,9,11,13,15\},\{2,6,10,14\},\{4,12\},\{8\}$	$\mathbb{D}_4 \wr \mathbb{D}_4$
9	$\{0\},\{1,7,9,15\},\{2,6,10,14\},\{3,5,11,13\},\{4,12\},\{8\}$	$\mathbb{S}_2 \wr \mathbb{D}_8$
10	$\{0\},\{1,3,5,7,9,15,11,13\},\{2,14\},\{4,12\},\{6,10\},\{8\}$	$\mathbb{D}_8 \wr \mathbb{S}_2$
11	$\{0\},\{1,7,9,15\},\{2,14\},\{3,5,11,13\},\{4,12\},\{6,10\},\{8\}$	$\mathbb{Z}_{16} \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$
12	$\{0\},\{1,15\},\{2,14\},\{3,13\},\{4,12\},\{5,11\},\{6,10\},\{7,9\},\{8\}$	$\mathbb{D}_{16}$

Métricas sobre $\mathbb{Z}_{17}$

N	Partición	G. de simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$	$\mathbb{S}_{17}$
2	$\{0\},\{1,2,4,8,9,13,15,16\},\{3,5,6,7,10,11,12,14\}$	$\mathbb{Z}_{17} \rtimes \mathbb{Z}_8$
3	$\{0\},\{1,4,13,16\},\{2,8,9,15\},\{3,5,12,14\},\{6,7,10,11\}$	$\mathbb{Z}_{17} \rtimes \mathbb{Z}_4$
4	$\{0\},\{1,16\},\{2,15\},\{3,14\},\{4,13\},\{5,12\},\{6,11\},\{7,10\},\{8,9\}$	$\mathbb{D}_{17}$

Métricas sobre $\mathbb{Z}_{18}$

N	Partición	G. de simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}$	$\mathbb{S}_{18}$
2	$\{0\},\{1,3,5,7,9,11,13,15,17\},\{2,4,6,8,10,12,14,16\}$	$\mathbb{S}_9 \wr \mathbb{S}_2$
3	$\{0\},\{1,2,3,4,5,6,7,8,10,11,12,13,14,15,16,17\},\{9\}$	$\mathbb{S}_2 \wr \mathbb{S}_9$
4	$\{0\},\{1,3,5,7,11,13,15,17\},\{2,4,6,8,10,12,14,16\},\{9\}$	$\mathbb{S}_2 \times \mathbb{S}_9$
5	$\{0\},\{1,2,4,5,7,8,10,11,13,14,16,17\},\{3,6,9,12,15\}$	$\mathbb{S}_6 \wr \mathbb{S}_3$
6	$\{0\},\{1,2,3,4,5,7,8,9,10,11,13,14,15,16,17\},\{6,12\}$	$\mathbb{S}_3 \wr \mathbb{S}_6$
7	$\{0\},\{1,2,4,5,7,8,10,11,13,14,16,17\},\{3,15,9\},\{6,12\}$	$\mathbb{S}_3 \wr \mathbb{S}_2 \wr \mathbb{S}_3$
8	$\{0\},\{1,3,5,7,9,11,13,15,17\},\{2,4,8,10,14,16\},\{6,12\}$	$\mathbb{S}_3 \wr \mathbb{S}_3 \wr \mathbb{S}_2$
9	$\{0\},\{1,2,4,5,7,8,10,11,13,14,16,17\},\{3,6,12,15\},\{9\}$	$\mathbb{S}_2 \wr \mathbb{S}_3 \wr \mathbb{S}_3$
10	$\{0\},\{1,5,7,11,13,17\},\{2,4,8,10,14,16\},\{3,9,15\},\{6,12\}$	$\mathbb{S}_3 \wr \mathbb{D}_6$
11	$\{0\},\{1,2,4,5,7,8,10,11,13,14,16,17\},\{3,15\},\{6,12\},\{9\}$	$\mathbb{D}_6 \wr \mathbb{S}_3$
12	$\{0\},\{1,8,10,17\},\{2,7,11,16\},\{3,6,12,15\},\{4,5,13,14\},\{9\}$	$\mathbb{S}_2 \wr \mathbb{D}_9$
13	$\{0\},\{1,3,5,7,9,11,13,15,17\},\{2,16\},\{4,14\},\{6,12\},\{8,10\}$	$\mathbb{D}_9 \wr \mathbb{S}_2$
14	$\{0\},\{1,5,7,11,13,17\},\{2,4,8,10,14,16\},\{3,15\},\{6,12\},\{9\}$	$\mathbb{S}_2 \times (\mathbb{S}_3 \wr \mathbb{S}_3)$
15	$\{0\},\{1,8,10,17\},\{2,11,7,16\},\{3,15\},\{4,5,13,14\},\{6,12\},\{9\}$	$(\mathbb{D}_6 \wr \mathbb{S}_3) \cap (\mathbb{S}_2 \wr \mathbb{D}_9)^*$
16	$\{0\},\{1,5,7,11,13,17\},\{2,16\},\{3,9,15\},\{4,14\},\{6,12\},\{8,10\}$	$(\mathbb{S}_3 \wr \mathbb{D}_6) \cap (\mathbb{D}_9 \wr \mathbb{S}_2)^*$
17	$\{0\},\{1,17\},\{2,16\},\{3,15\},\{4,14\},\{5,13\},\{6,12\},\{7,11\},\{8,10\},\{9\}$	$\mathbb{D}_{18}$

* Recordar que si bien la notación es de grupos abstractos, en realidad deben considerarse como grupos actuando sobre $\mathbb{Z}_{18}$, donde la intersección tiene sentido.

Métricas sobre $\mathbb{Z}_{19}$

N	Partición	G. de simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18\}$	$\mathbb{S}_{19}$
2	$\{0\},\{1,7,8,11,12,18\},\{2,3,5,14,16,17\},\{4,6,9,10,13,15\}$	$\mathbb{Z}_{19} \rtimes \mathbb{Z}_6$
3	$\{0\},\{1,18\},\{2,17\},\{3,16\},\{4,15\},\{5,14\},\{6,13\},\{7,12\},\{8,11\},\{9,10\}$	$\mathbb{D}_{19}$

Métricas sobre $\mathbb{Z}_{20}$

N	Partición	G. de simetrías
1	$\{0\},\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19\}$	$\mathbb{S}_{20}$
2	$\{0\},\{1,3,5,7,9,11,13,15,17,19\},\{2,4,6,8,10,12,14,16,18\}$	$\mathbb{S}_{10} \wr \mathbb{S}_2$
3	$\{0\},\{1,2,3,4,5,6,7,8,9,11,12,13,14,15,16,17,18,19\},\{10\}$	$\mathbb{S}_2 \wr \mathbb{S}_{10}$
4	$\{0\},\{1,2,3,5,6,7,9,10,11,13,14,15,17,18,19\},\{4,8,12,16\}$	$\mathbb{S}_5 \wr \mathbb{S}_4$
5	$\{0\},\{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19\},\{5,10,15\}$	$\mathbb{S}_4 \wr \mathbb{S}_5$
6	$\{0\},\{1,4,6,9,11,14,16,19\},\{2,3,7,8,12,13,17,18\},\{5,10,15\}$	$\mathbb{S}_4 \wr \mathbb{D}_5$
7	$\{0\},\{1,2,3,5,6,7,9,10,11,13,14,15,17,18,19\},\{4,16\},\{8,12\}$	$\mathbb{D}_5 \wr \mathbb{S}_4$
8	$\{0\},\{1,3,5,7,9,11,13,15,17,19\},\{2,4,6,8,12,14,16,18\},\{10\}$	$\mathbb{S}_2 \wr \mathbb{S}_5 \wr \mathbb{S}_2$
9	$\{0\},\{1,3,5,7,9,11,13,15,17,19\},\{2,6,10,14,18\},\{4,8,12,16\}$	$\mathbb{S}_5 \wr \mathbb{D}_4$
10	$\{0\},\{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19\},\{5,15\},\{10\}$	$\mathbb{D}_4 \wr \mathbb{S}_5$
11	$\{0\},\{1,3,7,9,11,13,17,19\},\{2,4,6,8,12,14,16,18\},\{5,15\},\{10\}$	$\mathbb{S}_2 \wr (\mathbb{S}_2 \times \mathbb{S}_5)$
12	$\{0\},\{1,3,5,7,9,11,13,15,17,19\},\{2,6,14,18\},\{4,8,12,16\},\{10\}$	$(\mathbb{S}_2 \times \mathbb{S}_5) \wr \mathbb{S}_2$
13	$\{0\},\{1,3,5,7,9,11,13,15,17,19\},\{2,8,12,18\},\{4,6,14,16\},\{10\}$	$\mathbb{S}_2 \wr \mathbb{D}_5 \wr \mathbb{S}_2$
14	$\{0\},\{1,4,6,9,11,14,16,19\},\{2,3,7,8,12,13,17,18\},\{5,15\},\{10\}$	$\mathbb{D}_4 \wr \mathbb{D}_5$
15	$\{0\},\{1,3,5,7,9,11,13,15,17,19\},\{2,6,10,14,18\},\{4,16\},\{8,12\}$	$\mathbb{D}_5 \wr \mathbb{D}_4$
16	$\{0\},\{1,9,11,19\},\{2,8,12,18\},\{3,7,13,17\},\{4,6,14,16\},\{5,15\},\{10\}$	$\mathbb{S}_2 \wr \mathbb{D}_{10}$
17	$\{0\},\{1,3,5,7,9,11,13,15,17,19\},\{2,18\},\{4,16\},\{6,14\},\{8,12\},\{10\}$	$\mathbb{D}_{10} \wr \mathbb{S}_2$
18	$\{0\},\{1,2,3,6,7,9,11,13,14,17,18,19\},\{4,8,12,16\},\{5,10,15\}$	$\mathbb{S}_4 \times \mathbb{S}_5$
19	$\{0\},\{1,3,7,9,11,13,17,19\},\{2,6,14,18\},\{4,8,12,16\},\{5,15\},\{10\}$	$\mathbb{D}_4 \times \mathbb{S}_5$
20	$\{0\},\{1,6,9,11,14,19\},\{2,3,7,13,17,18\},\{4,16\},\{5,10,15\},\{8,12\}$	$\mathbb{S}_4 \times \mathbb{D}_5$
21	$\{0\},\{1,9,11,19\},\{2,18\},\{3,7,13,17\},\{4,16\},\{5,15\},\{6,14\},\{8,12\},\{10\}$	$\mathbb{D}_4 \times \mathbb{D}_5$
22	$\{0\},\{1,19\},\{2,18\},\{3,17\},\{4,16\},\{5,15\},\{6,14\},\{7,13\},\{8,12\},\{9,11\},\{10\}$	$\mathbb{D}_{20}$

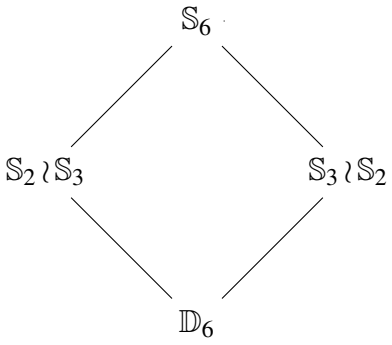
Cantidad de métricas schurianas sobre $\mathbb{Z}_n$

N	N de métricas	N de métricas schurianas
2	1	1
3	1	1
4	2	2
5	2	2
6	5	4
7	5	2
8	15	5
9	15	3
10	52	7
11	52	2
12	203	13
13	203	4
14	877	7
15	877	8
16	4140	12
17	4140	4
18	21147	17
19	21147	3
20	115975	22

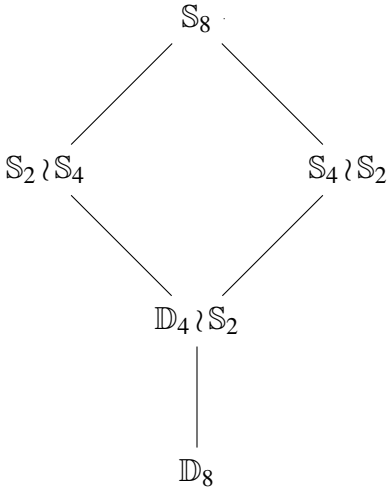
Apéndice B

Retículos de simetrías

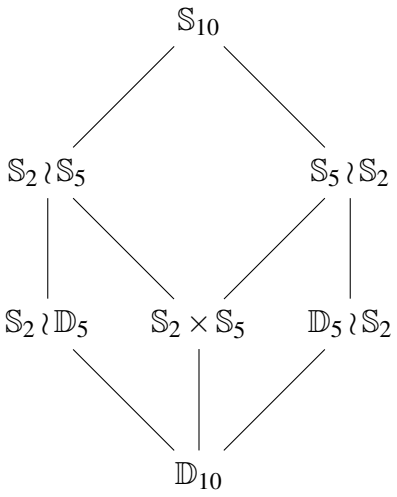
Retículo de simetrías de $\mathbb{Z}_6$



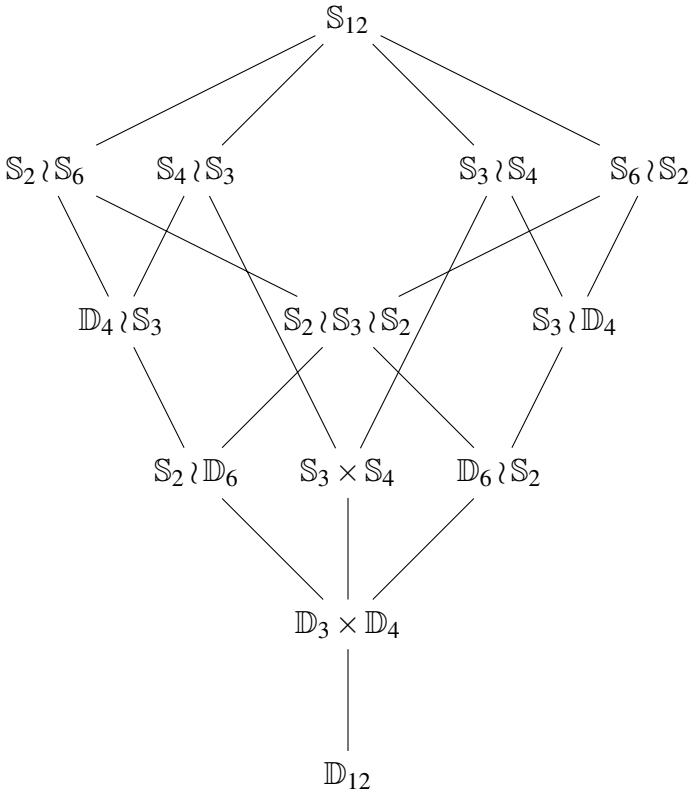
Retículo de simetrías de $\mathbb{Z}_8$



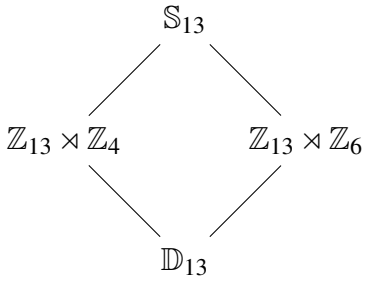
Retículo de simetrías de $\mathbb{Z}_{10}$



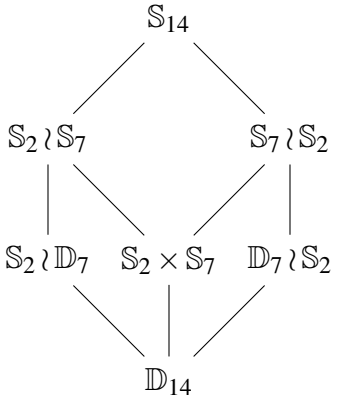
Retículo de simetrías de $\mathbb{Z}_{12}$



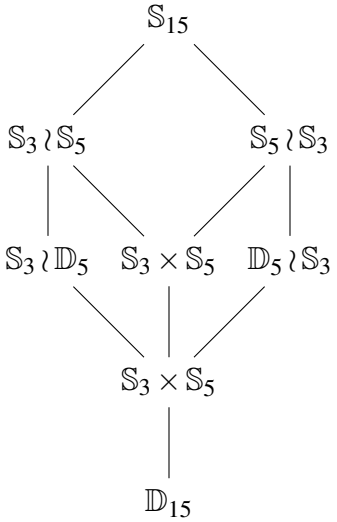
Retículo de simetrías de $\mathbb{Z}_{13}$



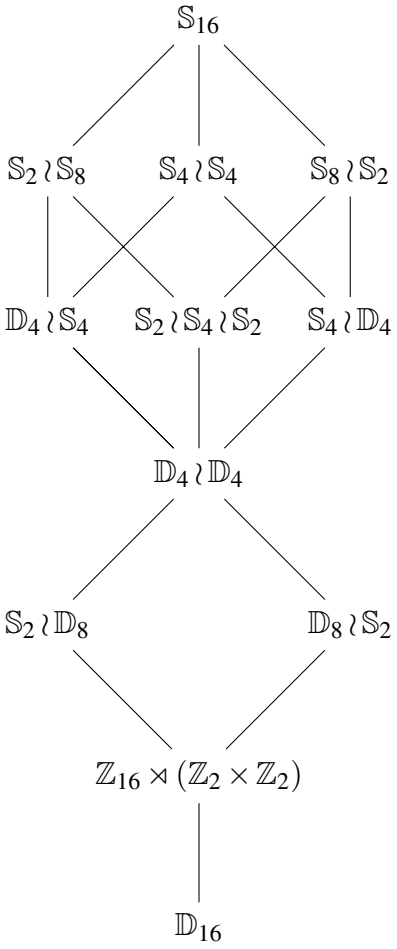
Retículo de simetrías de $\mathbb{Z}_{14}$



Retículo de simetrías de $\mathbb{Z}_{15}$



Retículo de simetrías de $\mathbb{Z}_{16}$



Bibliografía

[1] Marcelo Muniz Silva Alves y Sueli I. Rodrigues Costa. «Labelings of Lee and Hamming spaces». En: *Discrete Mathematics* 260.1-3 (2003), págs. 119-136. DOI: 10.1016/S0012-365X(02)00454-5. URL: https://doi.org/10.1016/S0012-365X(02)00454-5.

[2] Maria Carmen V. Amarra y Fidel R. Nemenzo. «On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$». En: *Appl. Math. Lett.* 21.11 (2008), págs. 1129-1133.

[3] Aleams Barra y Heide Gluesing-Luerssen. «MacWilliams Extension Theorems and the Local-Global Property for Codes over Rings». En: *CoRR* abs/1307.7159 (2013). arXiv: 1307.7159. URL: http://arxiv.org/abs/1307.7159.

[4] Sergey Bezzateev y Natalia A. Shekhunova. «Class of generalized Goppa codes perfect in weighted Hamming metric». En: *Des. Codes Cryptography* 66 (2013), págs. 391-399.

[5] R. C. Bose y Dale M. Mesner. «On Linear Associative Algebras Corresponding to Association Schemes of Partially Balanced Designs». En: *Ann. Math. Statist.* 30.1 (mar. de 1959), págs. 21-38. DOI: 10.1214/aoms/1177706356. URL: https://doi.org/10.1214/aoms/1177706356.

[6] R. C. Bose y T. Shimamoto. «Classification and Analysis of Partially Balanced Incomplete Block Designs with Two Associate Classes». En: *Journal of the American Statistical Association* 47.258 (1952), págs. 151-184. DOI: 10.1080/01621459.1952.10501161. eprint: http://www.tandfonline.com/doi/pdf/10.1080/01621459.1952.10501161.

[7] Richard A. Brualdi, Janine Smolin Graves y K.Mark Lawrence. «Codes with a poset metric». En: *Discrete Mathematics* 147.1 (1995), págs. 57-72. ISSN: 0012-365X. DOI: https://doi.org/10.1016/0012-365X(94)00228-B. URL: http://www.sciencedirect.com/science/article/pii/0012365X9400228B.

[8] Peter J. Cameron. «Automorphisms of graphs». En: *Topics in Algebraic Graph Theory*. 2004, págs. 137-155. ISBN: 0521801974.

[9] Claude Carlet. «$\mathbb{Z}_{p^k}$-Linear Codes». En: *IEEE Transactions on Information Theory* 44.4 (1998), págs. 1543-1547.

[10] Y. Cengellenmis. «On $(1-u^m)$-cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+\cdots+u^m\mathbb{F}_2$». En: *International Journal of Contempolary Mathematical Sciences* 218.4 (2009), págs. 987-992.

[11] H.L. Claasen y R.W. Goldbach. «A field-like property of finite rings». En: *Indagationes Mathematicae* 3.1 (1992), págs. 11-26. ISSN: 0019-3577. DOI: https://doi.org/10.1016/0019-3577(92)90024-F. URL: http://www.sciencedirect.com/science/article/pii/001935779290024F.

[12] I. Constantinescu y W. Heise. «A metric for codes over residue class rings.» English. Russian original. En: *Probl. Inf. Transm.* 33.3 (1997), págs. 208-213.

[13] Wikipedia contributors. *Holomorph (mathematics)*. [Online; accessed 06-March-2018]. 2018. URL: https://en.wikipedia.org/wiki/Holomorph_(mathematics).

[14] P. Delsarte. «An algebraic approach to the association schemes of coding theory». En: *Philips Res. Rep.* 10 (1973).

[15] P. Delsarte y V. I. Levenshtein. «Association Schemes and Coding Theory». En: *IEEE Trans. Inf. Theor.* 44.6 (sep. de 2006), págs. 2477-2504. ISSN: 0018-9448. DOI: 10.1109/18.720545. URL: http://dx.doi.org/10.1109/18.720545.

[16] S. Evdokimov, I. Kovács e I. Ponomarenko. «Characterization of cyclic Schur groups». En: *ArXiv e-prints* (nov. de 2011). arXiv: 1111.5216 [math.CO].

[17] S. Evdokimov e I. Ponomarenko. «Schur rings over a product of Galois rings». En: *ArXiv e-prints* (dic. de 2009). arXiv: 0912.1559 [math.CO].

[18] Sergei Evdokimov e Ilya Ponomarenko. «Coset closure of a circulant S-ring and schurity problem». En: *Journal of Algebra and Its Applications* 15.04 (2016), pág. 1650068. DOI: 10.1142/S0219498816500687. URL: https://www.worldscientific.com/doi/abs/10.1142/S0219498816500687.

[19] Roberto Frucht y Frank Harary. «On the corona of two graphs». En: *aequationes mathematicae* 4.3 (oct. de 1970), págs. 322-325. ISSN: 1420-8903. DOI: 10.1007/BF01844162. URL: https://doi.org/10.1007/BF01844162.

[20] Jr. G. D. Forney. «Transforms and groups». En: A. Vardy. *Codes, Curves and Signals: Common Threads in Communications*. Springer, Boston, MA, 1998, págs. 79-97.

[21] Heide Gluesing-Luerssen. «Fourier-Reflexive Partitions and MacWilliams Identities for Additive Codes». En: *CoRR* abs/1304.1207 (2013). arXiv: 1304.1207. URL: http://arxiv.org/abs/1304.1207.

[22] A. Roger Jr. Hammons y col. «The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes». En: *IEEE Transactions on Information Theory* 40.2 (1994), págs. 301-319.

[23] A. Hanaki e I. Miyamoto. «Classification of association schemes of small order». En: *Discrete Mathematics* 264.1 (2003). The 2000 Com2MaC Conference on Association Schemes, Codes and Designs, págs. 75-80. ISSN: 0012-365X. DOI: https://doi.org/10.1016/S0012-365X(02)00551-4. URL: http://www.sciencedirect.com/science/article/pii/S0012365X02005514.

[24] Y. Hirano. «On admissible rings». En: *Indagationes Mathematicae* 8.1 (1997), págs. 55-59. ISSN: 0019-3577. DOI: https://doi.org/10.1016/S0019-3577(97)83350-2. URL: http://www.sciencedirect.com/science/article/pii/S0019357797833502.

[25] T. Honold. «Characterization of finite Frobenius rings». En: *Archiv der Mathematik* 76.6 (jun. de 2001), págs. 406-415. ISSN: 1420-8938. DOI: 10.1007/PL00000451. URL: https://doi.org/10.1007/PL00000451.

[26] J. Y. Hyun, H. K. Kim y J. Rye Park. «The weighted poset metrics and directed graph metrics». En: *ArXiv e-prints* (mar. de 2017). arXiv: 1703.00139 [math.CO].

[27] Hyun Kwang Kim y Dong Yeol Oh. «A classification of posets admitting the MacWilliams identity». En: *IEEE Transactions on Information Theory* 51.4 (abr. de 2005), págs. 1424-1431. ISSN: 0018-9448. DOI: 10.1109/TIT.2005.844067.

[28] M. Kh. Klin y R. Poschel. «The Konig problem, the isomorphism problem for cyclic graphs and the method of schur rings». En: Algebraic Methods in Graph Theory (1978).

[29] T. Y. Lam. «[Graduate Texts in Mathematics] Lectures on Modules and Rings Volume 189 ||». En: vol. 10.1007/978-1-4612-0525-8. Springer-Verlag New York, 1999. ISBN: 978-1-4612-6802-4,978-1-4612-0525-8. DOI: 10.1007/978-1-4612-0525-8.

[30] Ka Hin Leung y Shing Hing Man. «On schur rings over cyclic groups». En: *Israel Journal of Mathematics* 106.1 (dic. de 1998), págs. 251-267. DOI: 10.1007/BF02773471. URL: https://doi.org/10.1007/BF02773471.

[31] Ka Hin Leung y Shing Hing Man. «On Schur Rings over Cyclic Groups, II». En: *Journal of Algebra* 183.2 (1996), págs. 273-285. ISSN: 0021-8693. DOI: https://doi.org/10.1006/jabr.1996.0220. URL: http://www.sciencedirect.com/science/article/pii/S0021869396902203.

[32] San Ling y Jason Thomas Blackford. «$\mathbb{Z}_{p^{k+1}}$-Linear codes.» En: *IEEE Transactions on Information Theory* 48.9 (2002), págs. 2592-2605.

[33] Marcelo Muniz Silva Alves Luciano Panek Marcelo Firer. «Classification of Niederreiter-Rosenbloom-Tsfasman block codes». En: *IEEE Transactions on Information Theory* 56 (2010), págs. 5207-5216.

[34] Marcelo Muniz Silva Alves Luciano Panek Marcelo Firer. «Symmetry groups of Rosenbloom-Tsfasman spaces». En: *Discrete Mathematics* 309.4 (2009), págs. 763-771. DOI: 10.1016/j.disc.2008.01.013.

[35] Marcelo Firer Luciano Viana Felix. «Canonical- systematic form for codes in hierarchical poset metrics». En: *Advances in Mathematics of Communications* 6 (2012), pág. 315. ISSN: 1930-5346. DOI: 10.3934/amc.2012.6.315.

[36] S. L. Ma. «On association schemes, schur rings, strongly regular graphs and partial difference sets». En: Ars Combin. 27 (1989), págs. 211-220.

[37] Roberto Machado, Jerry Pinheiro y Marcelo Firer. «Characterization of Metrics Induced by Hierarchical Posets». En: *IEEE Transactions on Information Theory* PP (ago. de 2015).

[38] F.J. MacWilliams y N.J.A. Sloane. *The Theory of Error-Correcting Codes*. 2nd. North-holland Publishing Company, 1978.

[39] Andrew Misseldine. *Algebraic and Combinatorial Properties of Schur Rings over Cyclic Groups*. Mayo de 2014.

[40] Marcelo Muniz y Sueli I. R. Costa. «Labelings of Lee and Hamming Spaces». En: *Discrete Math.* 260.1-3 (ene. de 2003), págs. 119-136. ISSN: 0012-365X. DOI: 10.1016/S0012-365X(02)00454-5. URL: http://dx.doi.org/10.1016/S0012-365X(02)00454-5.

[41] M.E. Muzychuk. «On the Structure of Basic Sets of Schur Rings over Cyclic Groups». En: *Journal of Algebra* 169.2 (1994), págs. 655-678. ISSN: 0021-8693. DOI: https://doi.org/10.1006/jabr.1994.1302. URL: http://www.sciencedirect.com/science/article/pii/S0021869384713020.

[42] Mikhail Muzychuk. «Adam's conjecture is true in the square-free case». En: *Journal of Combinatorial Theory, Series A* 72.1 (1995), págs. 118-134.

[43] Mikhail Muzychuk e Ilia Ponomarenko. «Schur rings». En: *European Journal of Combinatorics* 30.6 (2009). Association Schemes: Ideas and Perspectives, págs. 1526-1539. ISSN: 0195-6698. DOI: https://doi.org/10.1016/j.ejc.2008.11.006. URL: http://www.sciencedirect.com/science/article/pii/S019566980800245X.

[44] A. A. Nechaev. «Kerdock code in a cyclic form». En: *Discrete Mathematics and Applications* 1 (4 1991), págs. 365-384. DOI: 10.1515/dma.1991.1.4.365.

[45] Dong Yeol Oh. «Poset metrics admitting association schemes and a new proof of MacWilliams identity». En: *Journal of the Korean Mathematical Society* 50.5 (2013), págs. 917-931. DOI: 10.4134/JKMS.2013.50.5.917.

[46] Dong Yeol Oh. «Poset metrics admitting association schemes and a new proof of Macwilliams identity». En: *Journal of the Korean Mathematical Society* 50.5 (2013), págs. 917-931.

[47] Mehmet Ozen e Irfan Siap. «On The Structure and Decoding of Linear Codes with Respect to the Rosenbloom-Tsfasman Metric». En: *Selcuk Journal of Applied Mathematics* (ene. de 2004).

[48] P. Camion. «Codes and association schemes». En: V. S. Pless y W. C. Huffman. *Handbook of Coding Theory, Vol. II*. Elsevier, 1998, págs. 1441-1566.

[49] P. Delsarte. «An algebraic approach to the association schemes of coding theory». En: *Philips Res. Repts. Suppl* (1973), págs. 79-97.

[50] Luciano Panek y Nayene Michele Paião Panek. «Symmetry Group of Ordered Hamming Block Space». En: *CoRR* abs/1705.09987 (2017). eprint: 1705.09987. URL: http://arxiv.org/abs/1705.09987.

[51] Luciano Panek y col. «Groups of linear isometries on poset structures». En: *Discrete Mathematics* 308.18 (2008), págs. 4116-4123. ISSN: 0012-365X. DOI: https://doi.org/10.1016/j.disc.2007.08.001. URL: http://www.sciencedirect.com/science/article/pii/S0012365X07006061.

[52] W. Park y A. Barg. «The ordered Hamming metric and ordered symmetric channels». En: *2011 IEEE International Symposium on Information Theory Proceedings*. Jul. de 2011, págs. 2283-2287. DOI: 10.1109/ISIT.2011.6033968.

[53] Woomyoung Park y Alexander Barg. «Linear ordered codes, shape enumarators and parallel channels». En: *Communication, Control, and Computing (Allerton), 2010 48th Annual Allerton Conference on*. IEEE. 2010, págs. 361-367.

[54] I. Ponomarenko y G. Ryabov. «Abelian Schur groups of odd order». En: *ArXiv e-prints* (oct. de 2017). arXiv: 1710.10908 [math.GR].

[55] Jian-Fa Qian, Li-Na Zhang y Shi-Xin Zhu. «$(1+u)$ constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$». En: *Appl. Math. Lett.* 19.8 (2006), págs. 820-823.

[56] Jian-Fa Qian, Li-Na Zhang y Shi-Xin Zhu. «Constacyclic and Cyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$». En: *IEICE Transactions* 89-A.6 (2006), págs. 1863-1865.

[57] Steven Roman. *Introduction to coding and information theory.* Undergraduate texts in mathematics. Springer, 1997, págs. I-XIII, 1-323.

[58] M. M. Skriganov S. T. Dougherty. «MacWilliams duality and the Rosenbloom–Tsfasman metric». En: *Mosc. Math. J.* 2.1 (2002), págs. 81-97.

[59] Ana Salagean-Mandache. «On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$». En: *IEEE Transactions on Information Theory* 45.6 (1999), págs. 2146-2148.

[60] R. Schmidt. *Subgroup Lattices of Groups*. De Gruyter Expositions in Mathematics. De Gruyter, 1994. ISBN: 9783110868647. URL: https://books.google.com.ar/books?id=SVq8Ax-V3vsC.

[61] Claude E. Shannon. «A Mathematical Theory of Communication». En: *Bell System Technical Journal* 27 (1948), págs. 379-423.

[62] Amit K. Sharma y Anuradha Sharma. «MacWilliams identities for weight enumerators with respect to the RT metric». En: *Discrete Mathematics, Algorithms and Applications* 06.02 (2014), pág. 1450030. DOI: 10.1142/S179383091450030X.

[63] *The On-Line Encyclopedia of Integer Sequences*. Sequence A000110. Bell or exponential numbers: number of ways to partition a set of n labeled elements. URL: https://oeis.org/A000110.

[64] T. Ericson V. A. Zinov'ev. «On Fourier-Invariant Partitions of Finite Abelian Groups and the MacWilliams Identity for Group Codes». En: *Probl. Peredachi Inf.* 32.1 (1996). URL: http://mi.mathnet.ru/ppi328.

[65] Jay A. Wood. «Duality For Modules Over Finite Rings And Applications To Coding Theory». En: *Americ. J. of Math.* 121 (1999), págs. 555-575.

[66] Jay A. Wood y col. «Applications of Finite Frobenius Rings to the Foundations of Algebraic Coding Theory». En: (2011).

[67] Bahattin Yildiz y Zeynep Odemis Ozger. «A generalization of the Lee weight to $\mathbb{Z}_{p^k}$». En: *TWMS Journal of Applied and Engineering Mathematics* 2.2 (2012), pág. 145.

[68] V. A. Zinoviev y T. Ericson. «Fourier-invariant Pairs of Partitions of Finite Abelian Groups and Association Schemes». En: *Probl. Inf. Transm.* 45.3 (sep. de 2009), págs. 221-231. ISSN: 0032-9460. DOI: 10.1134/S003294600903003X. URL: http://dx.doi.org/10.1134/S003294600903003X.

[69] Matan Ziv-Av. «Enumeration of Schur Rings Over Small Groups». En: *Computer Algebra in Scientific Computing*. Ed. por Vladimir P. Gerdt y col. Cham: Springer International Publishing, 2014, págs. 491-500. ISBN: 978-3-319-10515-4.